FIG.1

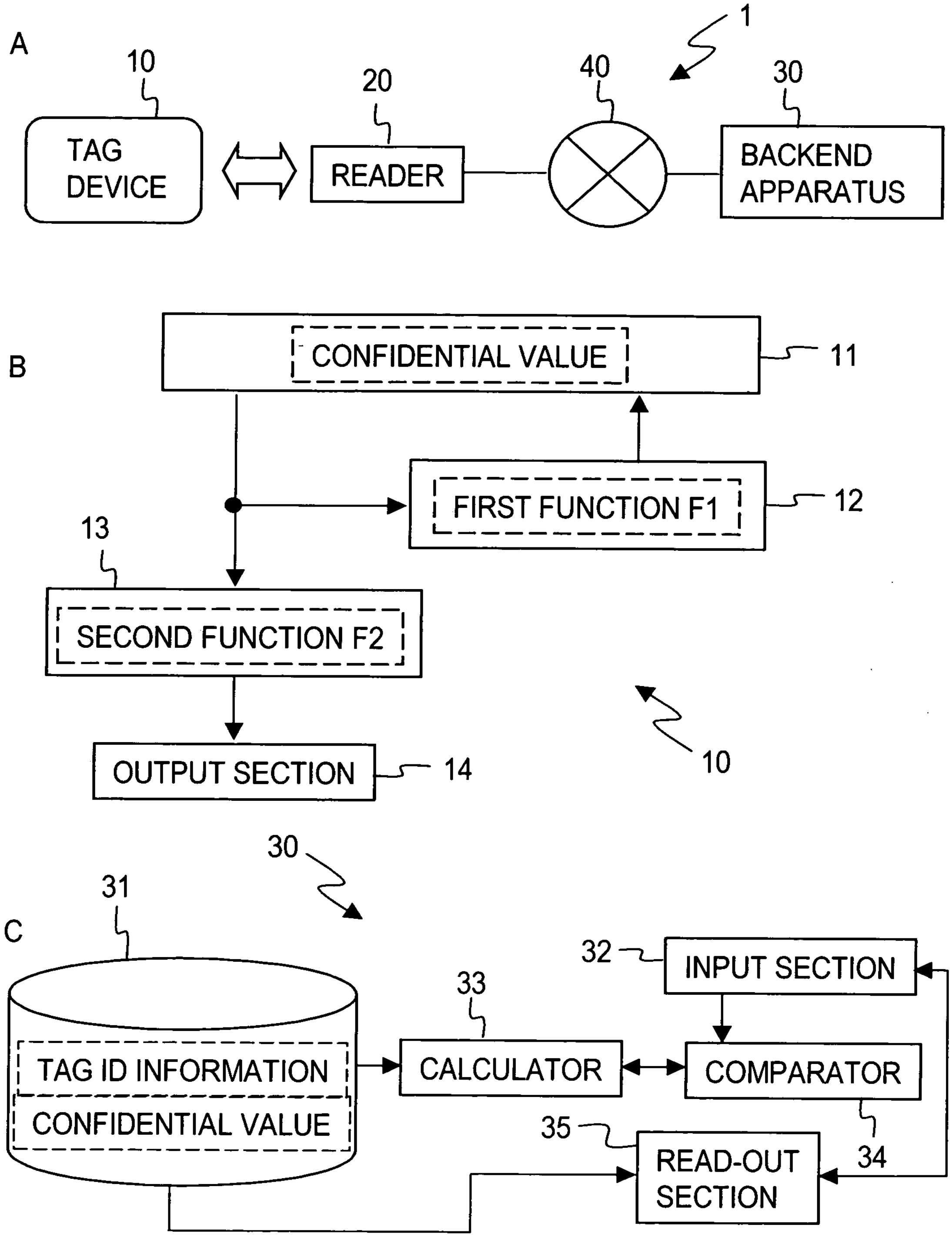

A
1
10
TAG DEVICE
20
READER
40
30
BACKEND APPARATUS
B
CONFIDENTIAL VALUE
11
FIRST FUNCTION F1
12
13
SECOND FUNCTION F2
OUTPUT SECTION
14
10
30
31
C
TAG ID INFORMATION
CONFIDENTIAL VALUE
33
CALCULATOR
32
INPUT SECTION
COMPARATOR
34
35
READ-OUT SECTION

FIG.2

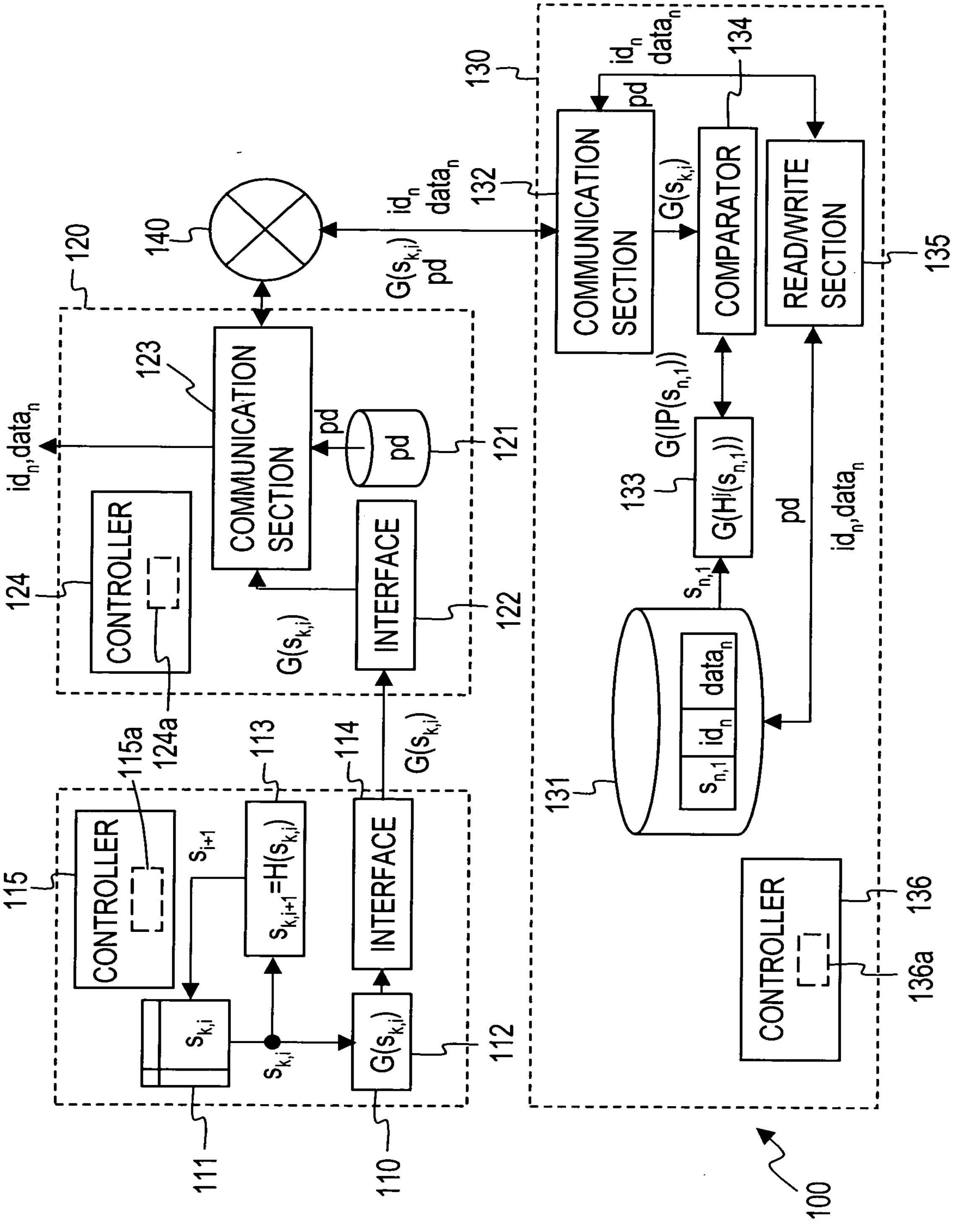
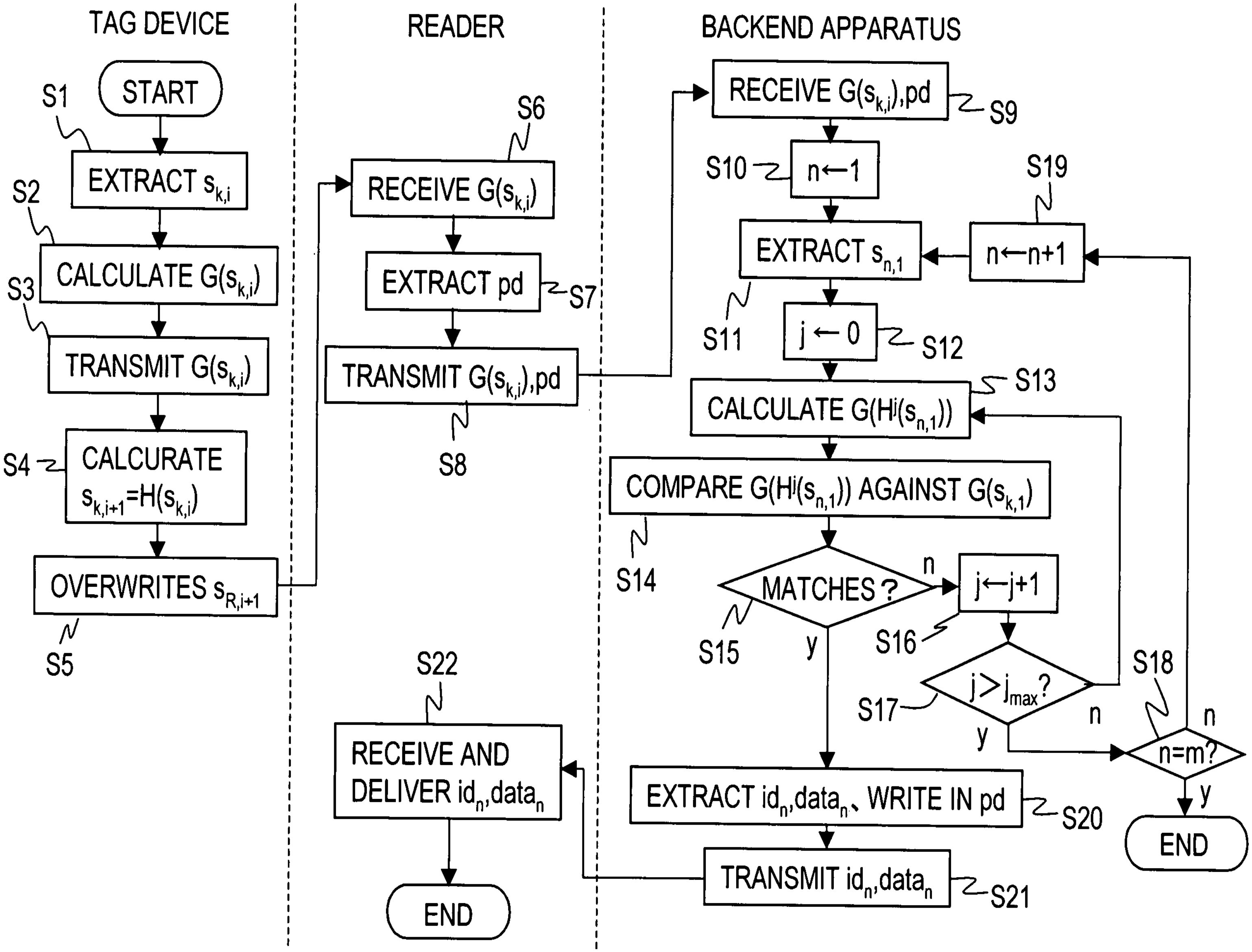

100
110
111
112
113
114
115
115a
CONTROLLER
$s_{k,i}$
$s_{k,i+1}=H(s_{k,i})$
s_{i+1}
$G(s_{k,i})$
INTERFACE
120
121
122
123
124
124a
CONTROLLER
COMMUNICATION SECTION
INTERFACE
pd
$id_n,data_n$
140
$G(s_{k,i})$ pd
id_n $data_n$
130
131
132
133
134
135
136
136a
COMMUNICATION SECTION
COMPARATOR
READ/WRITE SECTION
CONTROLLER
$G(Hi(s_{n,1}))$
$G(IP(s_{n,1}))$
$s_{n,1}$
id_n
$data_n$
pd
$id_n,data_n$

FIG.3


TAG DEVICE
READER
BACKEND APPARATUS
START
S1
EXTRACT $s_{k,i}$
S2
CALCULATE $G(s_{k,i})$
S3
TRANSMIT $G(s_{k,i})$
S4
CALCURATE $s_{k,i+1}=H(s_{k,i})$
OVERWRITES $s_{R,i+1}$
S5
S6
RECEIVE $G(s_{k,i})$
EXTRACT pd
S7
TRANSMIT $G(s_{k,i})$,pd
S8
S22
RECEIVE AND DELIVER id_n,$data_n$
END
RECEIVE $G(s_{k,i})$,pd
S9
S10
n←1
S19
n←n+1
EXTRACT $s_{n,1}$
S11
j ← 0
S12
S13
CALCULATE $G(H^j(s_{n,1}))$
COMPARE $G(H^j(s_{n,1}))$ AGAINST $G(s_{k,1})$
S14
MATCHES ?
n
j←j+1
S15
y
S16
S18
$j>j_{max}$?
S17
n
y
n
n=m?
y
EXTRACT id_n,$data_n$、WRITE IN pd
S20
END
TRANSMIT id_n,$data_n$
S21

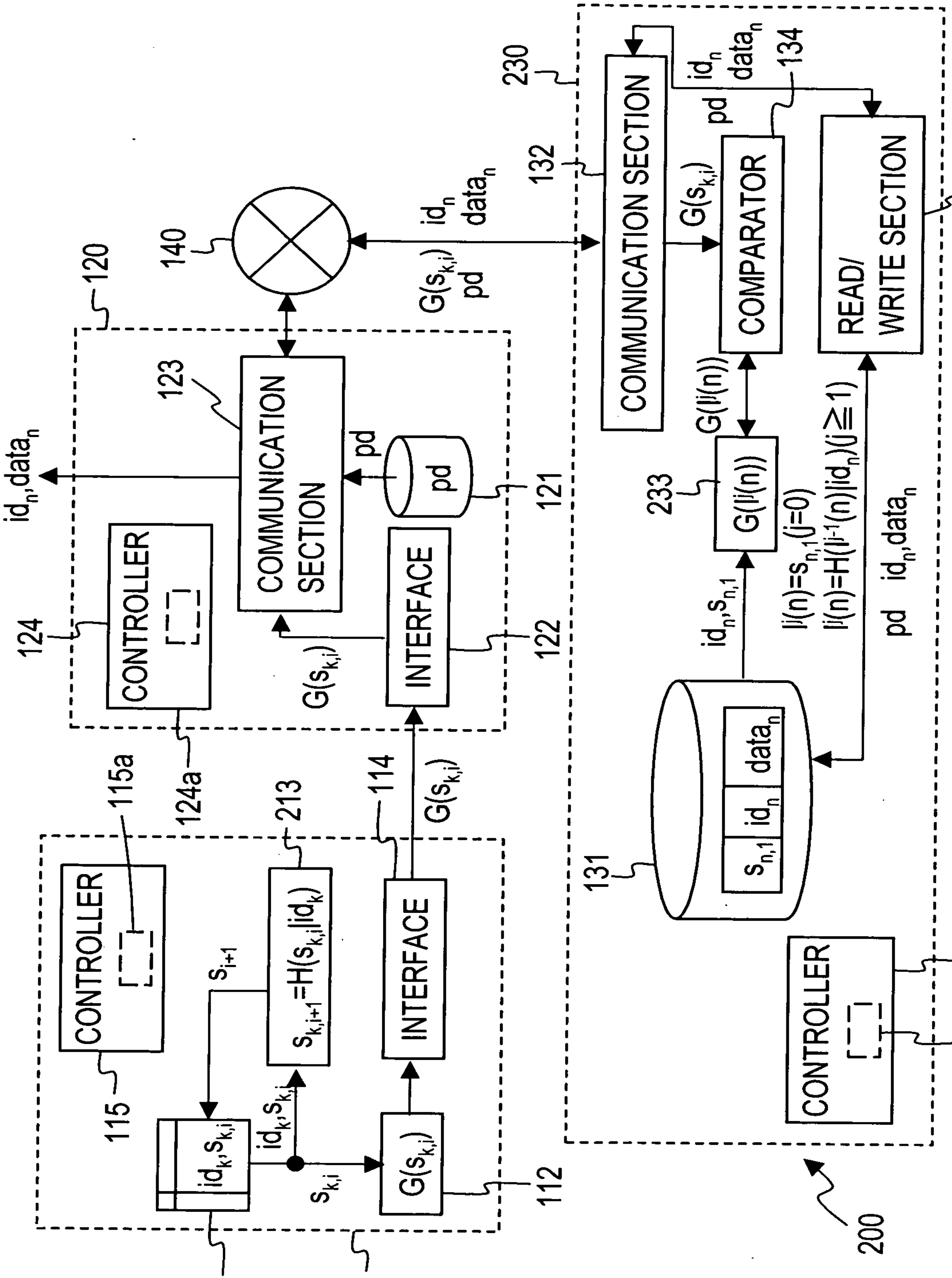


FIG.4

200
210
211
$id_k, s_{k,i}$
115
CONTROLLER
115a
$s_{k,i}$
$id_k, s_{k,i}$
s_{i+1}
$s_{k,i+1}=H(s_{k,i}||id_k)$
213
$G(s_{k,i})$
112
INTERFACE
114
$G(s_{k,i})$
120
124
CONTROLLER
124a
COMMUNICATION SECTION
123
INTERFACE
122
$G(s_{k,i})$
pd
pd
121
$id_n, data_n$
140
$G(s_{k,i})$
pd
id_n
$data_n$
230
COMMUNICATION SECTION
132
$G(s_{k,i})$
pd
id_n
$data_n$
COMPARATOR
134
READ/ WRITE SECTION
135
$G(l^j(n))$
$G(l^j(n))$
233
$id_n, s_{n,1}$
$l^j(n)=s_{n,1}(j=0)$
$l^j(n)=H(l^{j-1}(n)||id_n)(j\geqq1)$
pd $id_n, data_n$
131
$s_{n,1}$
id_n
$data_n$
CONTROLLER
136
136a

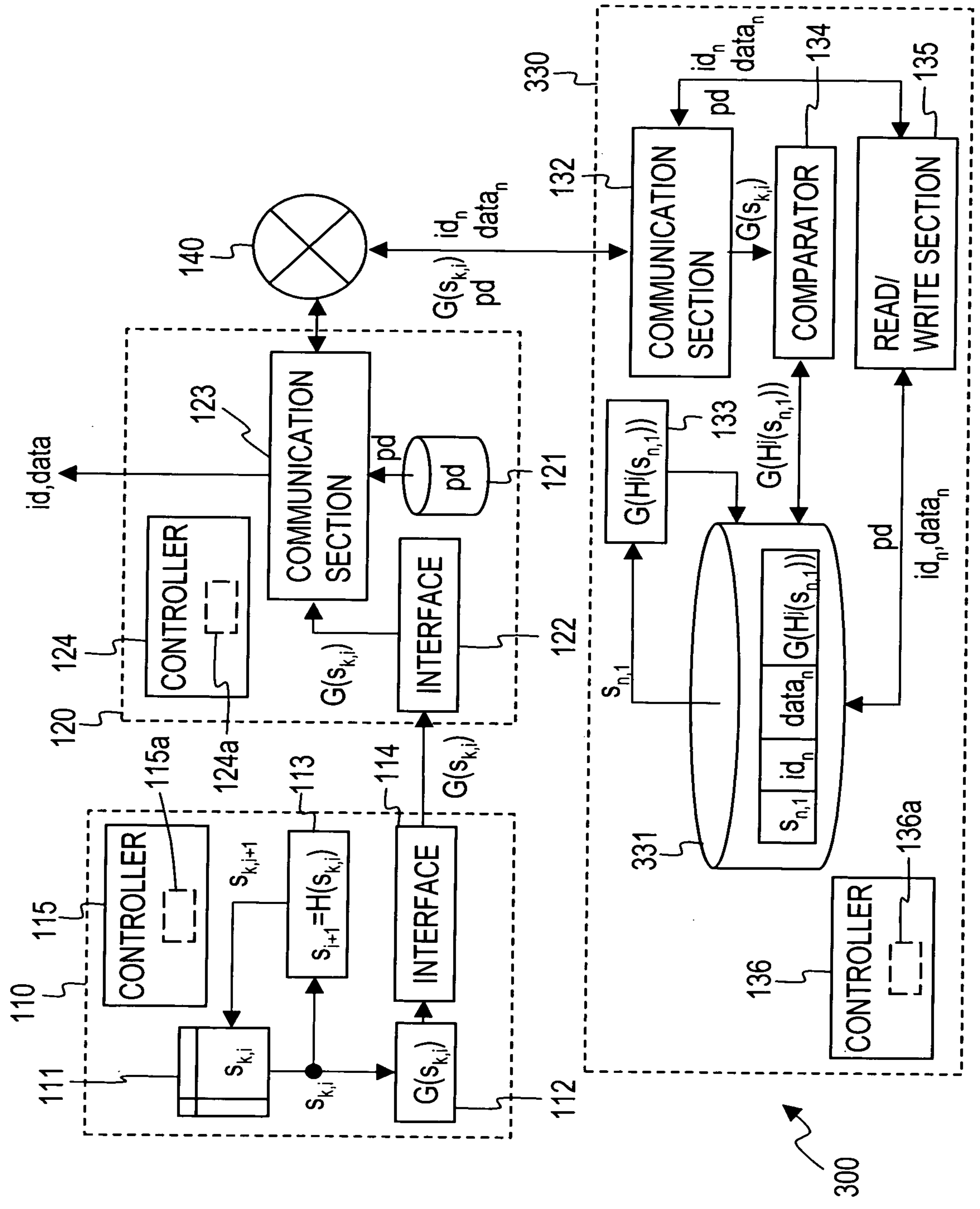
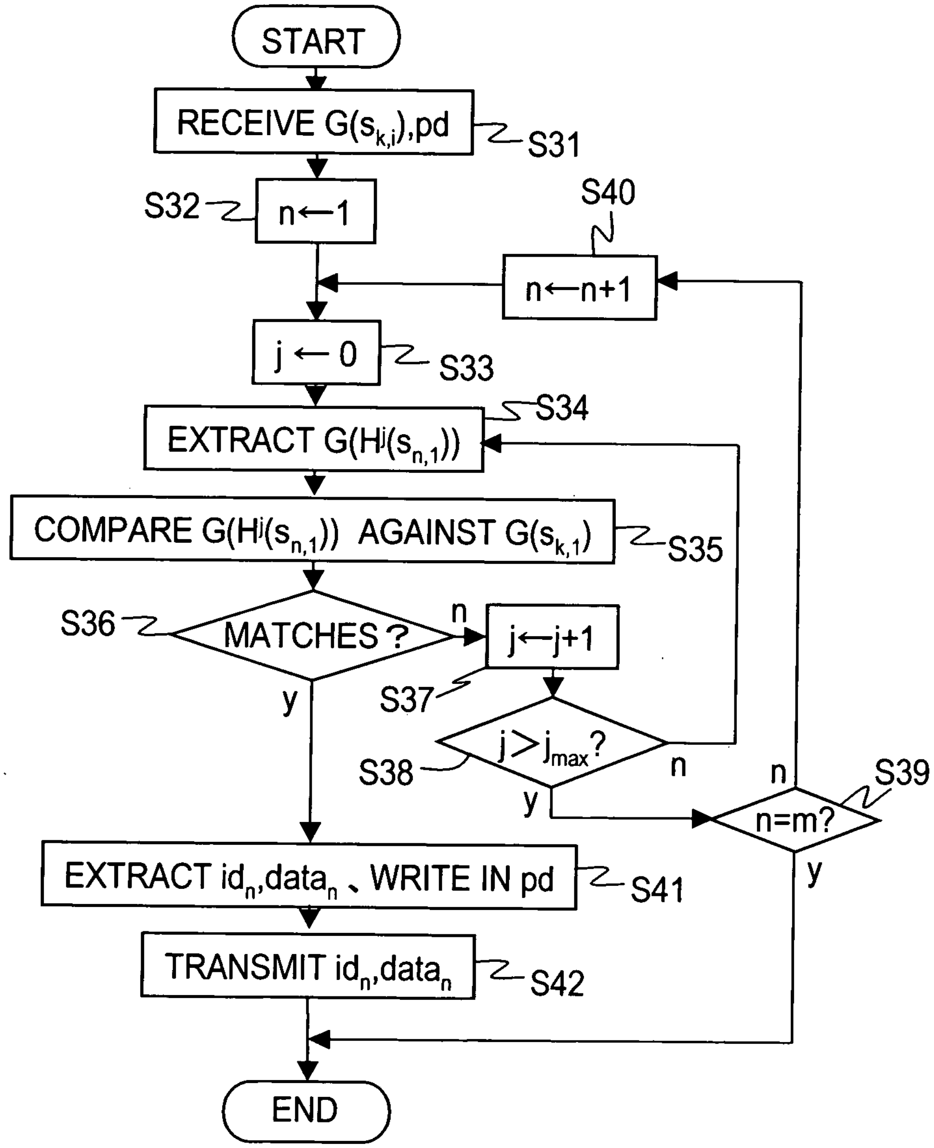

110
111
$s_{k,i}$
$s_{k,i}$
112
$G(s_{k,i})$
115
CONTROLLER
115a
$s_{k,i+1}$
$s_{i+1}=H(s_{k,i})$
113
114
INTERFACE
$G(s_{k,i})$
120
124
CONTROLLER
124a
$G(s_{k,i})$
INTERFACE
122
COMMUNICATION SECTION
123
pd
pd
121
id,data
140
$G(s_{k,i})$
pd
id_n
$data_n$
330
132
COMMUNICATION SECTION
$G(s_{k,i})$
COMPARATOR
134
READ/ WRITE SECTION
135
pd
id_n
$data_n$
$G(H^j(s_{n,1}))$
133
$G(H^j(s_{n,1}))$
$s_{n,1}$
$s_{n,1}$
id_n
$data_n$
$G(H^j(s_{n,1}))$
pd
$id_n,data_n$
331
136
CONTROLLER
136a
300

FIG.5

FIG.6


START
RECEIVE $G(s_{k,i})$,pd
S31
S32
n←1
S40
n←n+1
j ← 0
S33
S34
EXTRACT $G(H^j(s_{n,1}))$
COMPARE $G(H^j(s_{n,1}))$ AGAINST $G(s_{k,1})$
S35
S36
MATCHES ?
n
j←j+1
y
S37
$j > j_{max}$?
S38
n
n
S39
y
n=m?
y
EXTRACT id_n,$data_n$ 、WRITE IN pd
S41
TRANSMIT id_n,$data_n$
S42
END

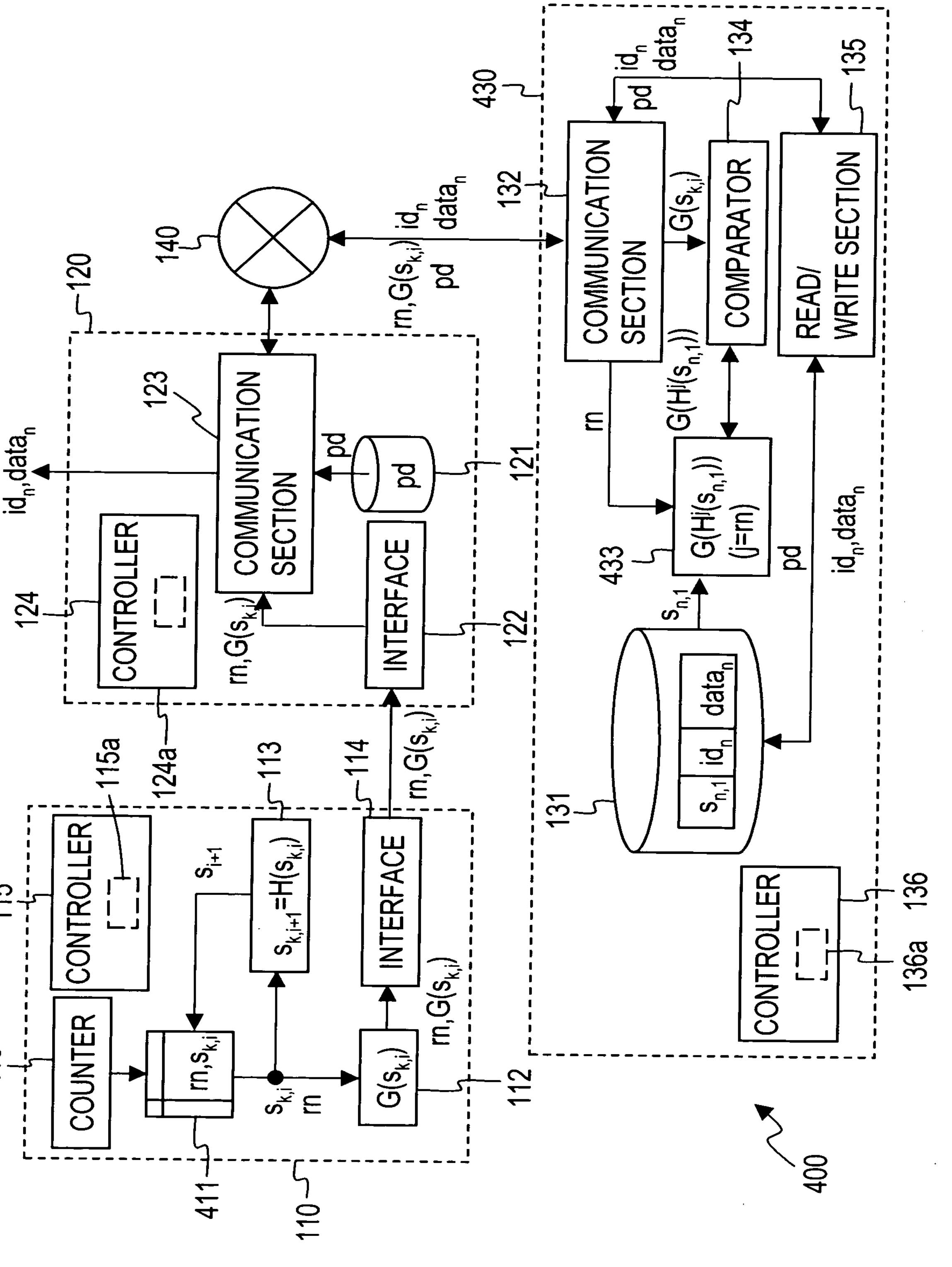
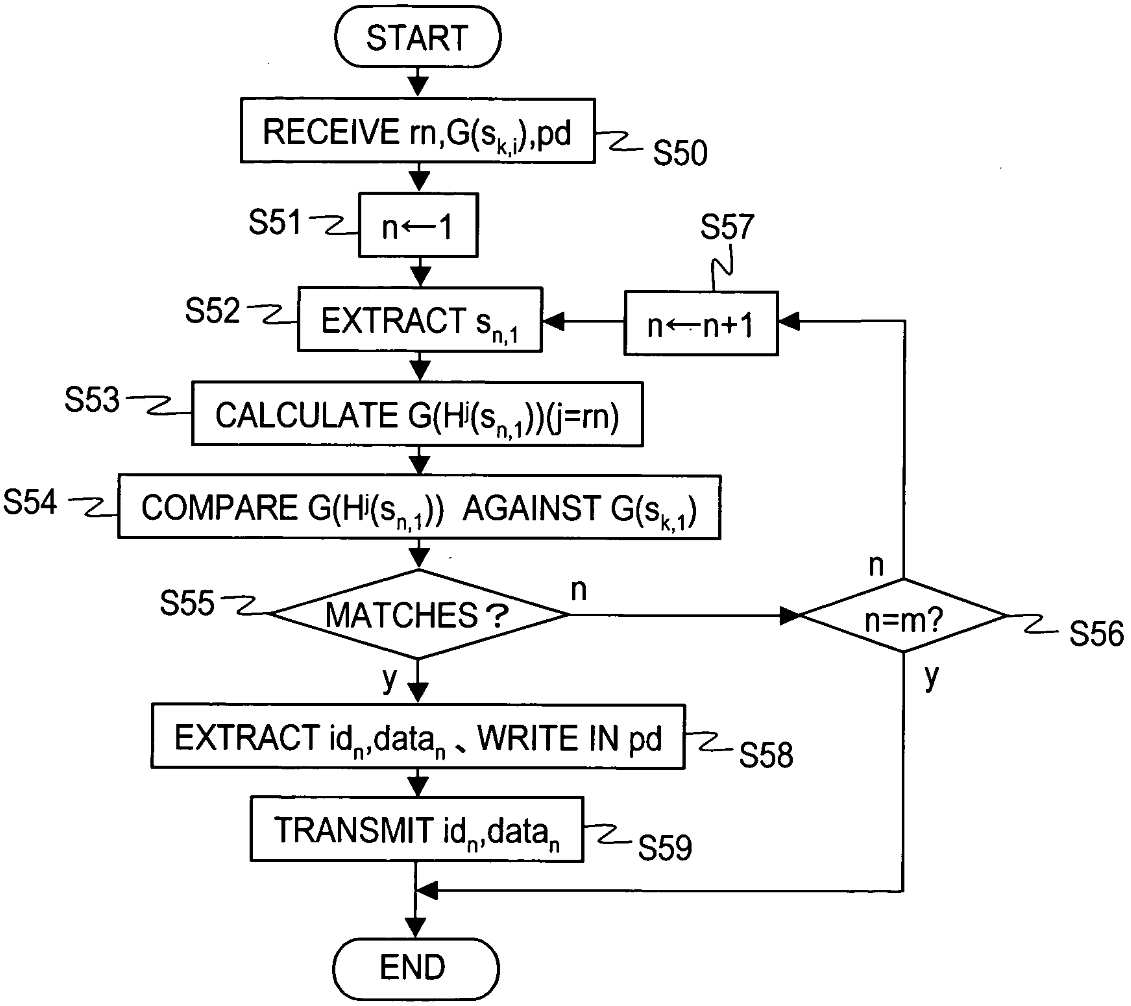

400
110
416
COUNTER
411
rn,$s_{k,i}$
115
CONTROLLER
115a
113
$s_{k,i+1}$=H($s_{k,i}$)
s_{i+1}
$s_{k,i}$
rn
G($s_{k,i}$)
112
114
INTERFACE
rn,G($s_{k,i}$)
124a
120
124
CONTROLLER
123
COMMUNICATION SECTION
id_n,$data_n$
pd
121
122
INTERFACE
rn,G($s_{k,i}$)
140
rn,G($s_{k,i}$) id_n $data_n$ pd
430
132
COMMUNICATION SECTION
G($s_{k,i}$)
134
COMPARATOR
135
READ/ WRITE SECTION
pd id_n $data_n$
rn
G(Hj($s_{n,1}$))
433
G(Hj($s_{n,1}$)) (j=rn)
$s_{n,1}$
pd
id_n,$data_n$
131
$s_{n,1}$
id_n
$data_n$
136
CONTROLLER
136a

FIG.7

FIG.8


START
RECEIVE rn,$G(s_{k,i})$,pd
S50
S51
n←1
S57
S52
EXTRACT $s_{n,1}$
n←n+1
S53
CALCULATE $G(H^j(s_{n,1}))(j=rn)$
S54
COMPARE $G(H^j(s_{n,1}))$ AGAINST $G(s_{k,1})$
S55
MATCHES？
n
n
n=m?
S56
y
y
EXTRACT id_n,$data_n$、WRITE IN pd
S58
TRANSMIT id_n,$data_n$
S59
END

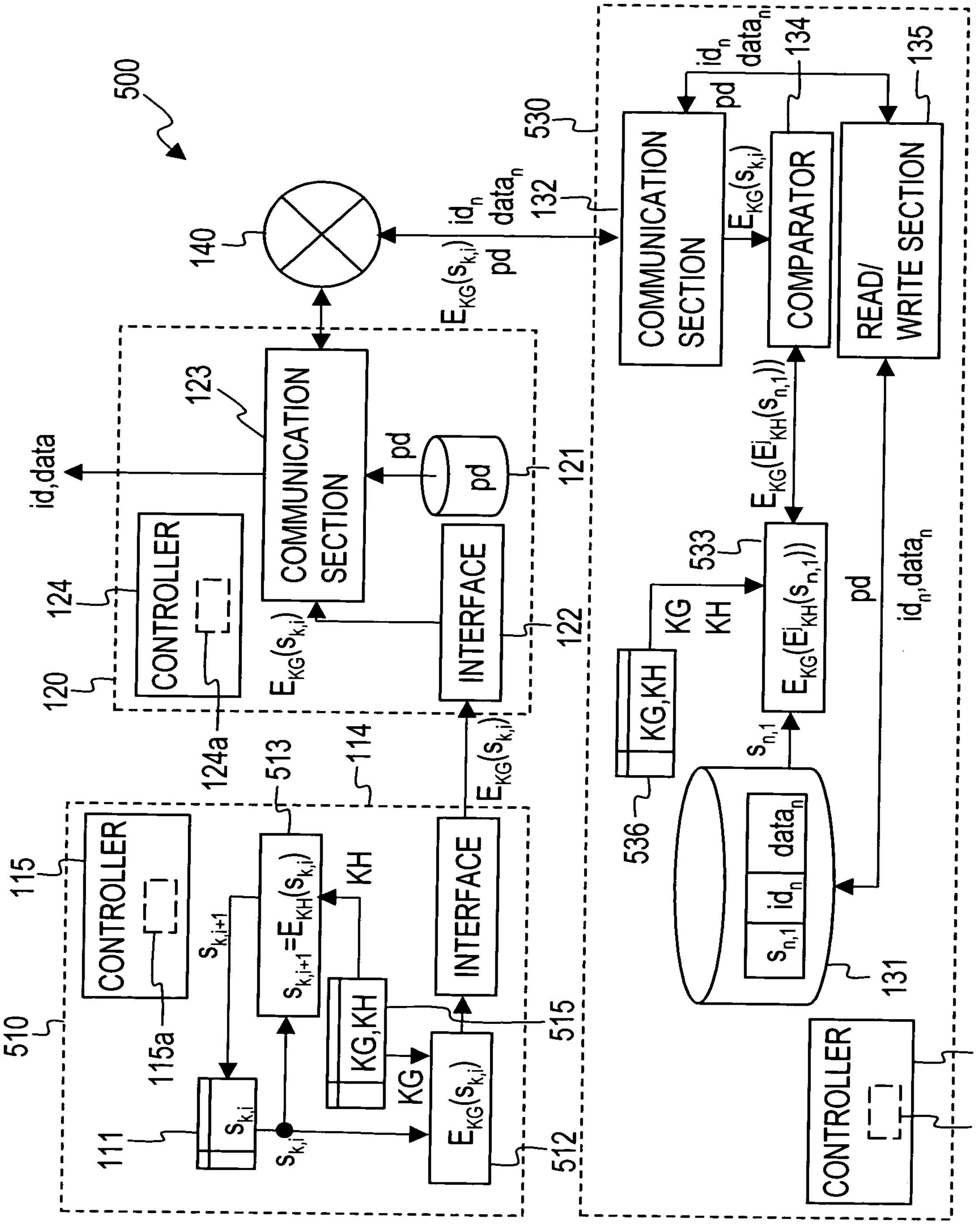

500
140
510
111
$s_{k,i}$
$s_{k,i}$
$s_{k,i+1}$
$s_{k,i+1}=E_{KH}(s_{k,i})$
KH
KG,KH
KG
$E_{KG}(s_{k,i})$
512
515
INTERFACE
CONTROLLER
115
115a
513
114
$E_{KG}(s_{k,i})$
120
CONTROLLER
124
124a
$E_{KG}(s_{k,i})$
INTERFACE
122
COMMUNICATION SECTION
123
pd
pd
121
id,data
$E_{KG}(s_{k,i})$
pd
id_n
$data_n$
530
132
COMMUNICATION SECTION
id_n
$data_n$
pd
134
$E_{KG}(s_{k,i})$
COMPARATOR
135
READ/ WRITE SECTION
$E_{KG}(E_{i_{KH}}(s_{n,1}))$
533
KG
KH
KG,KH
536
$E_{KG}(E_{i_{KH}}(s_{n,1}))$
$s_{n,1}$
pd
$id_n,data_n$
$s_{n,1}$
id_n
$data_n$
131
CONTROLLER
136
136a

FIG.9

FIG.10

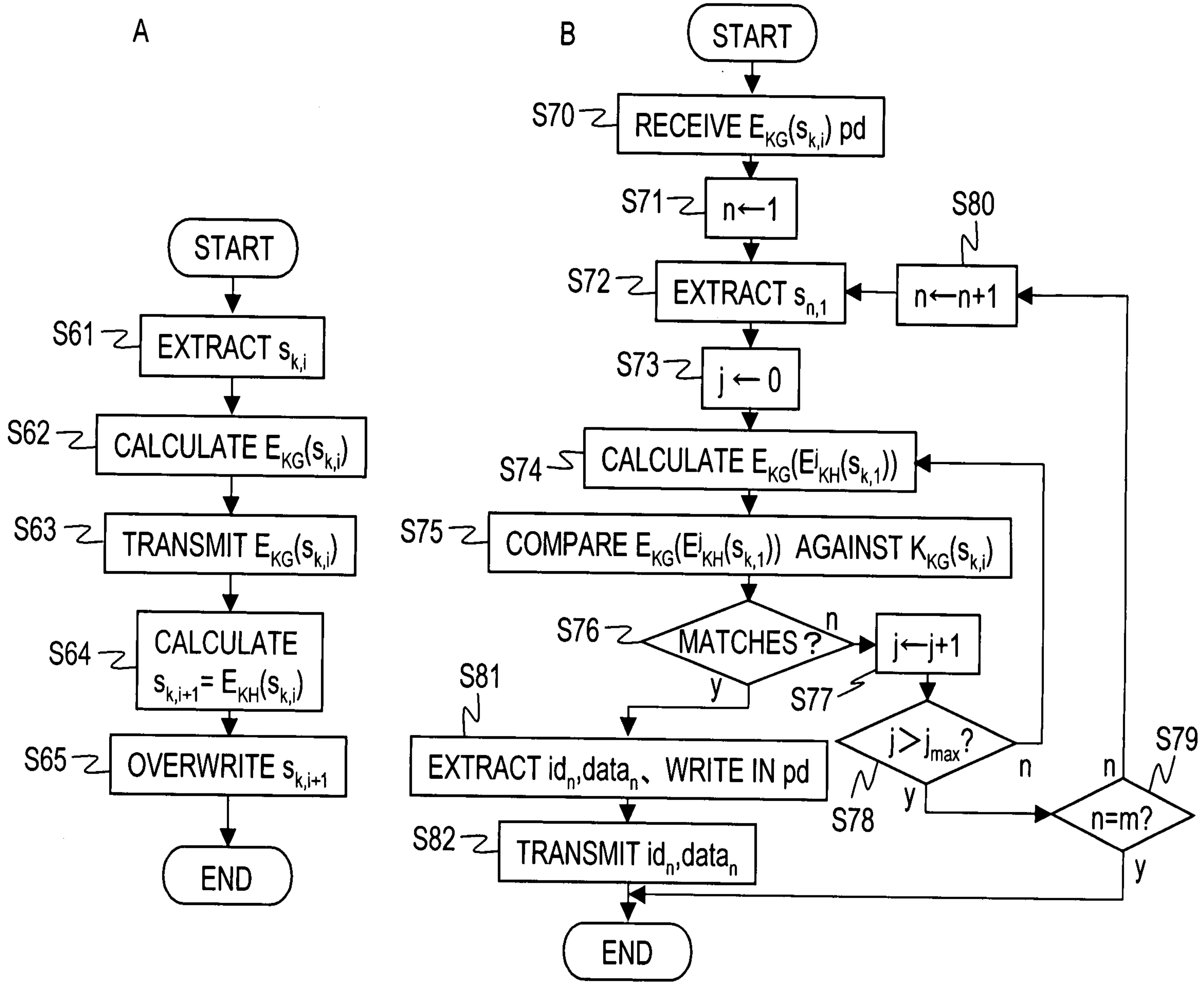

A
START
S61
EXTRACT $s_{k,i}$
S62
CALCULATE $E_{KG}(s_{k,i})$
S63
TRANSMIT $E_{KG}(s_{k,i})$
S64
CALCULATE $s_{k,i+1}=E_{KH}(s_{k,i})$
S65
OVERWRITE $s_{k,i+1}$
END
B
START
S70
RECEIVE $E_{KG}(s_{k,i})$ pd
S71
n←1
S72
EXTRACT $s_{n,1}$
S80
n←n+1
S73
j ← 0
S74
CALCULATE $E_{KG}(Ej_{KH}(s_{k,1}))$
S75
COMPARE $E_{KG}(Ej_{KH}(s_{k,1}))$ AGAINST $K_{KG}(s_{k,i})$
S76
MATCHES ?
n
y
j←j+1
S77
$j>j_{max}$?
n
y
S78
S79
n=m?
n
y
S81
EXTRACT id_n,$data_n$、WRITE IN pd
S82
TRANSMIT id_n,$data_n$
END

FIG.11

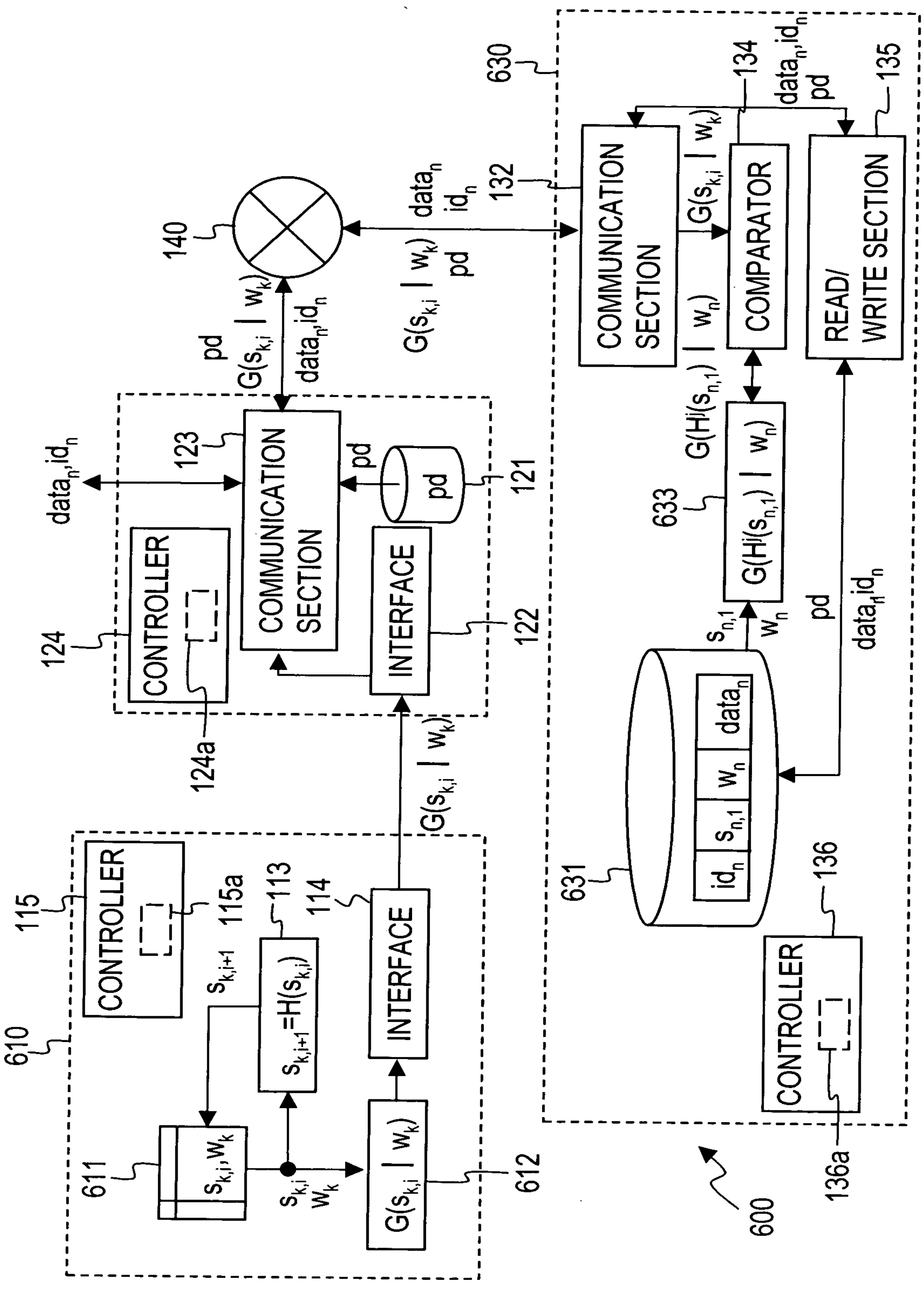

610
611
$s_{k,i}, w_k$
$s_{k,i}$
w_k
612
$G(s_{k,i} \mid w_k)$
113
$s_{k,i+1}=H(s_{k,i})$
$s_{k,i+1}$
115
CONTROLLER
115a
114
INTERFACE
$G(s_{k,i} \mid w_k)$
124
CONTROLLER
124a
123
COMMUNICATION SECTION
122
INTERFACE
121
pd
pd
$data_n, id_n$
pd
$G(s_{k,i} \mid w_k)$
$data_n, id_n$
140
$G(s_{k,i} \mid w_k)$
pd
$data_n$
id_n
630
132
COMMUNICATION SECTION
$G(s_{k,i} \mid w_k)$
134
COMPARATOR
$G(H^j(s_{n,1}) \mid w_n)$
$data_n, id_n$
pd
135
READ/ WRITE SECTION
633
$G(H^j(s_{n,1}) \mid w_n)$
$s_{n,1}$
w_n
pd
$data_n, id_n$
631
id_n
$s_{n,1}$
w_n
$data_n$
136
CONTROLLER
136a
600

FIG.12

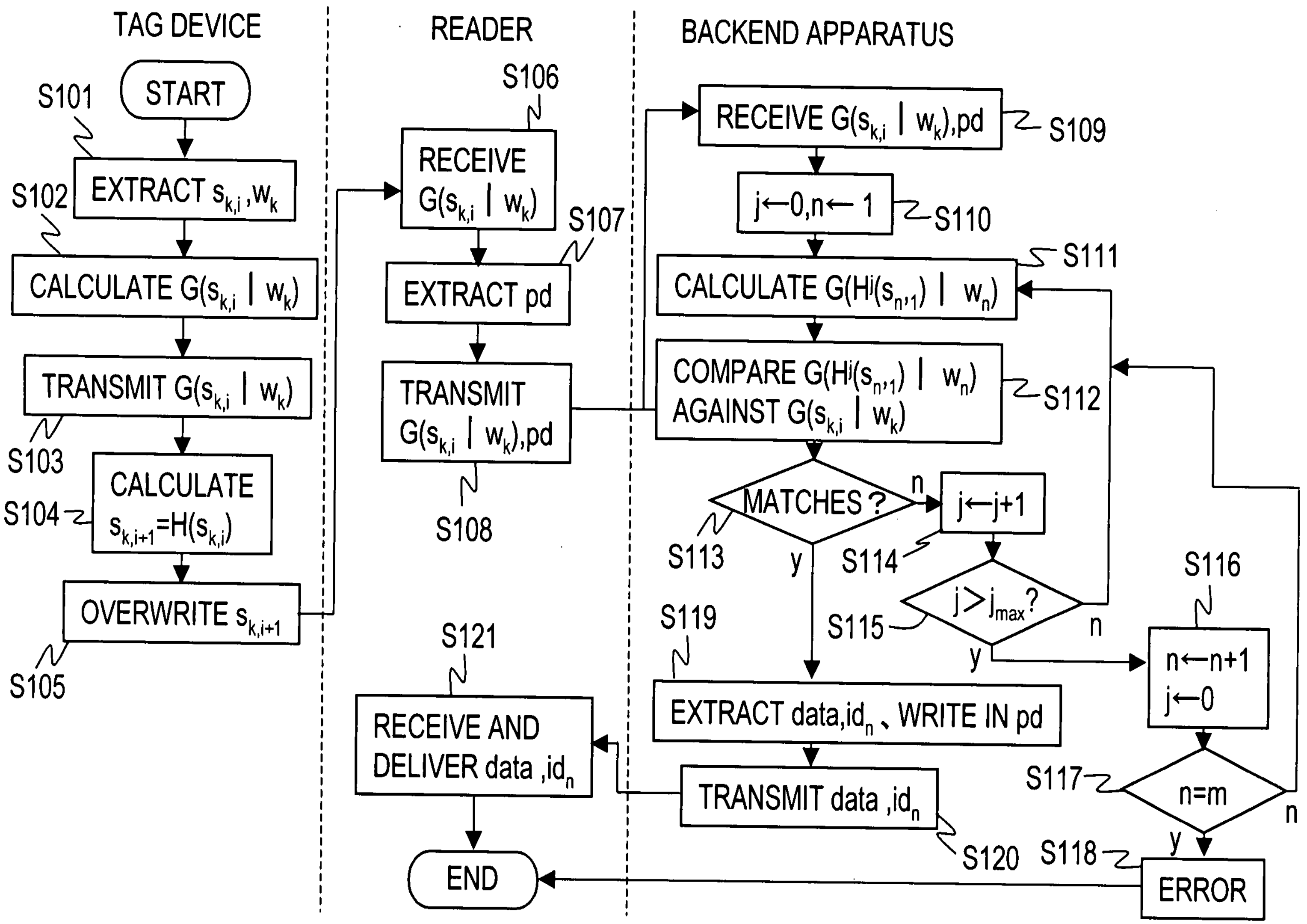

TAG DEVICE
READER
BACKEND APPARATUS
START
S101
EXTRACT $s_{k,i}$,w_k
S102
CALCULATE G($s_{k,i}$ | w_k)
TRANSMIT G($s_{k,i}$ | w_k)
S103
CALCULATE
$s_{k,i+1}$=H($s_{k,i}$)
S104
OVERWRITE $s_{k,i+1}$
S105
S106
RECEIVE
G($s_{k,i}$ | w_k)
S107
EXTRACT pd
TRANSMIT
G($s_{k,i}$ | w_k),pd
S108
RECEIVE G($s_{k,i}$ | w_k),pd
S109
j←0,n← 1
S110
S111
CALCULATE G(H^j($s_{n,1}$) | w_n)
COMPARE G(H^j($s_{n,1}$) | w_n)
AGAINST G($s_{k,i}$ | w_k)
S112
MATCHES ?
S113
n
y
j←j+1
S114
j>j_{max}?
S115
n
y
S116
n←n+1
j←0
S117
n=m
n
y
S118
ERROR
S119
EXTRACT data,id_n 、WRITE IN pd
TRANSMIT data ,id_n
S120
S121
RECEIVE AND
DELIVER data ,id_n
END

FIG.13

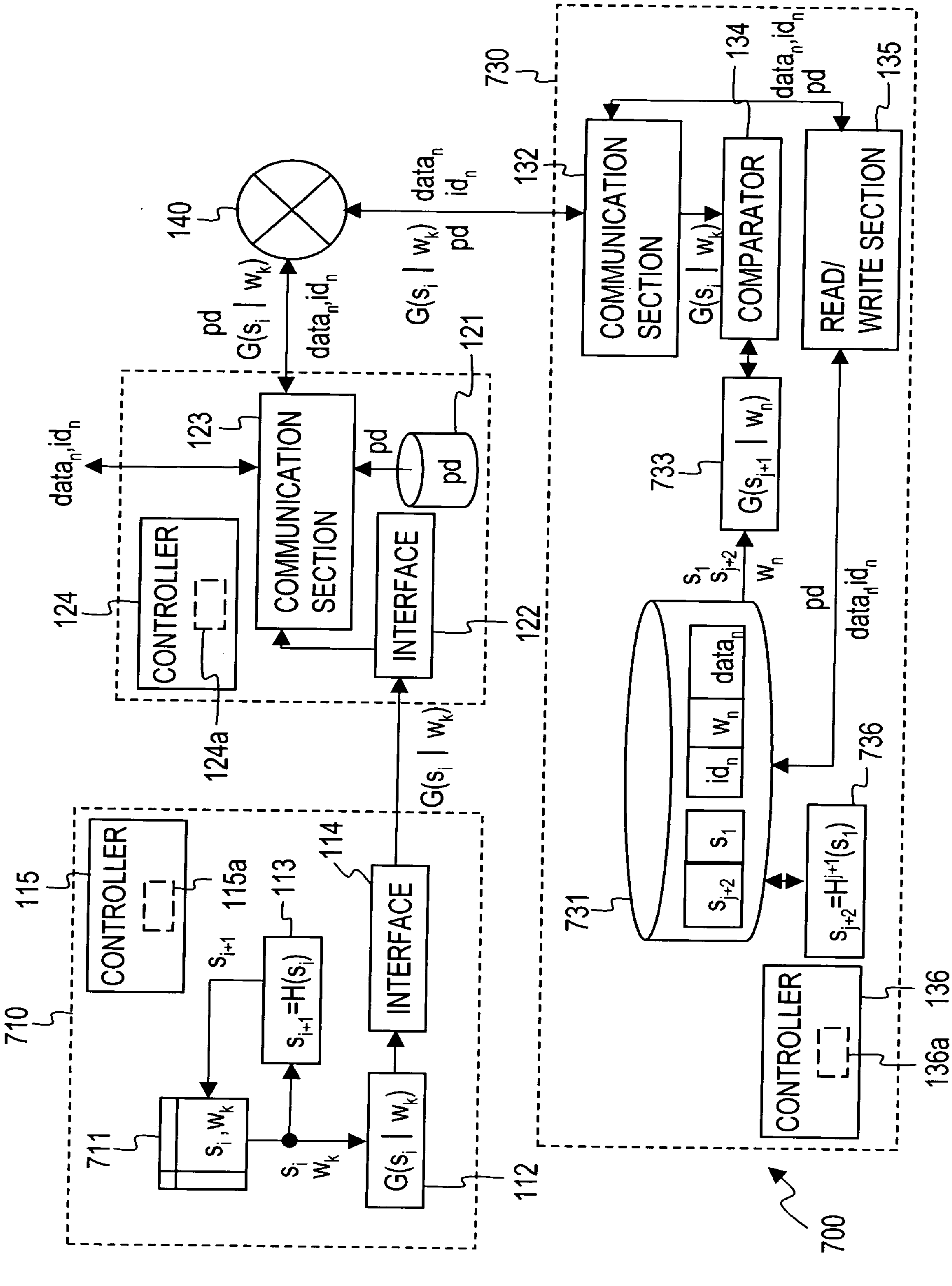

700
710
711
s_i, w_k
s_i w_k
112
$G(s_i \mid w_k)$
113
$s_{i+1}=H(s_i)$
s_{i+1}
114
INTERFACE
115
CONTROLLER
115a
$G(s_i \mid w_k)$
124
CONTROLLER
124a
123
COMMUNICATION SECTION
122
INTERFACE
121
pd
pd
$data_n, id_n$
pd
$G(s_i \mid w_k)$
$data_n, id_n$
140
$G(s_i \mid w_k)$
pd
$data_n$
id_n
730
132
COMMUNICATION SECTION
$G(s_i \mid w_k)$
COMPARATOR
134
$data_n, id_n$
pd
135
READ/ WRITE SECTION
733
$G(s_{j+1} \mid w_n)$
s_1
s_{j+2}
w_n
pd
$data_n id_n$
731
s_{j+2}
s_1
id_n
w_n
$data_n$
736
$s_{j+2}=H^{j+1}(s_1)$
136
CONTROLLER
136a

FIG.14

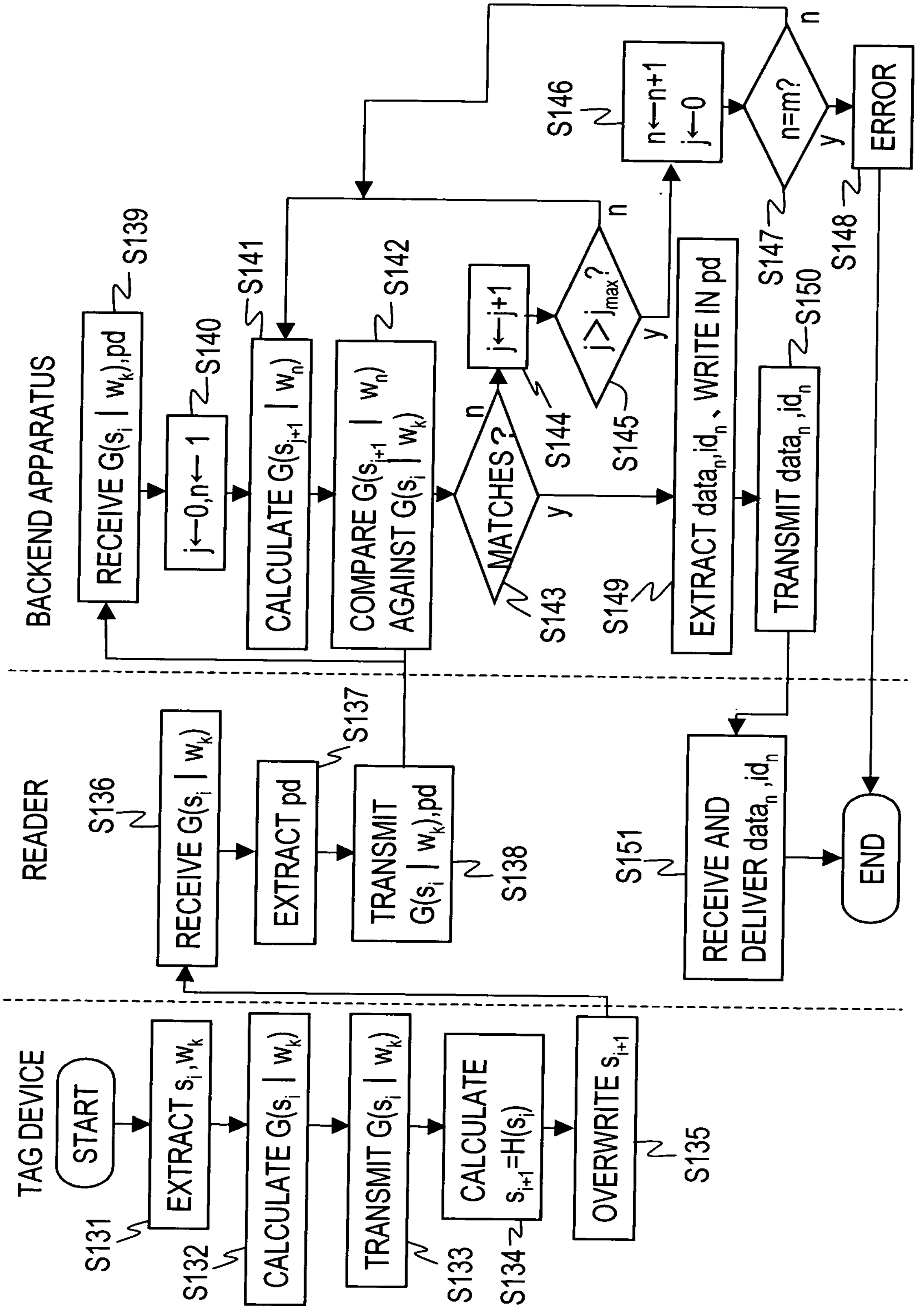

TAG DEVICE
START
EXTRACT s_i, w_k
S131
CALCULATE $G(s_i \mid w_k)$
S132
TRANSMIT $G(s_i \mid w_k)$
S133
CALCULATE $s_{i+1}=H(s_i)$
S134
OVERWRITE s_{i+1}
S135
READER
RECEIVE $G(s_i \mid w_k)$
S136
EXTRACT pd
S137
TRANSMIT $G(s_i \mid w_k)$,pd
S138
RECEIVE AND DELIVER $data_n$, id_n
S151
END
BACKEND APPARATUS
RECEIVE $G(s_i \mid w_k)$,pd
S139
$j \leftarrow 0, n \leftarrow 1$
S140
CALCULATE $G(s_{j+1} \mid w_n)$
S141
COMPARE $G(s_{j+1} \mid w_n)$ AGAINST $G(s_i \mid w_k)$
S142
MATCHES ?
S143
y
n
$j \leftarrow j+1$
S144
$j > j_{max}$?
S145
y
n
$n \leftarrow n+1$
$j \leftarrow 0$
S146
n=m?
S147
y
n
ERROR
S148
EXTRACT $data_n$, id_n , WRITE IN pd
S149
TRANSMIT $data_n$, id_n
S150

FIG.15

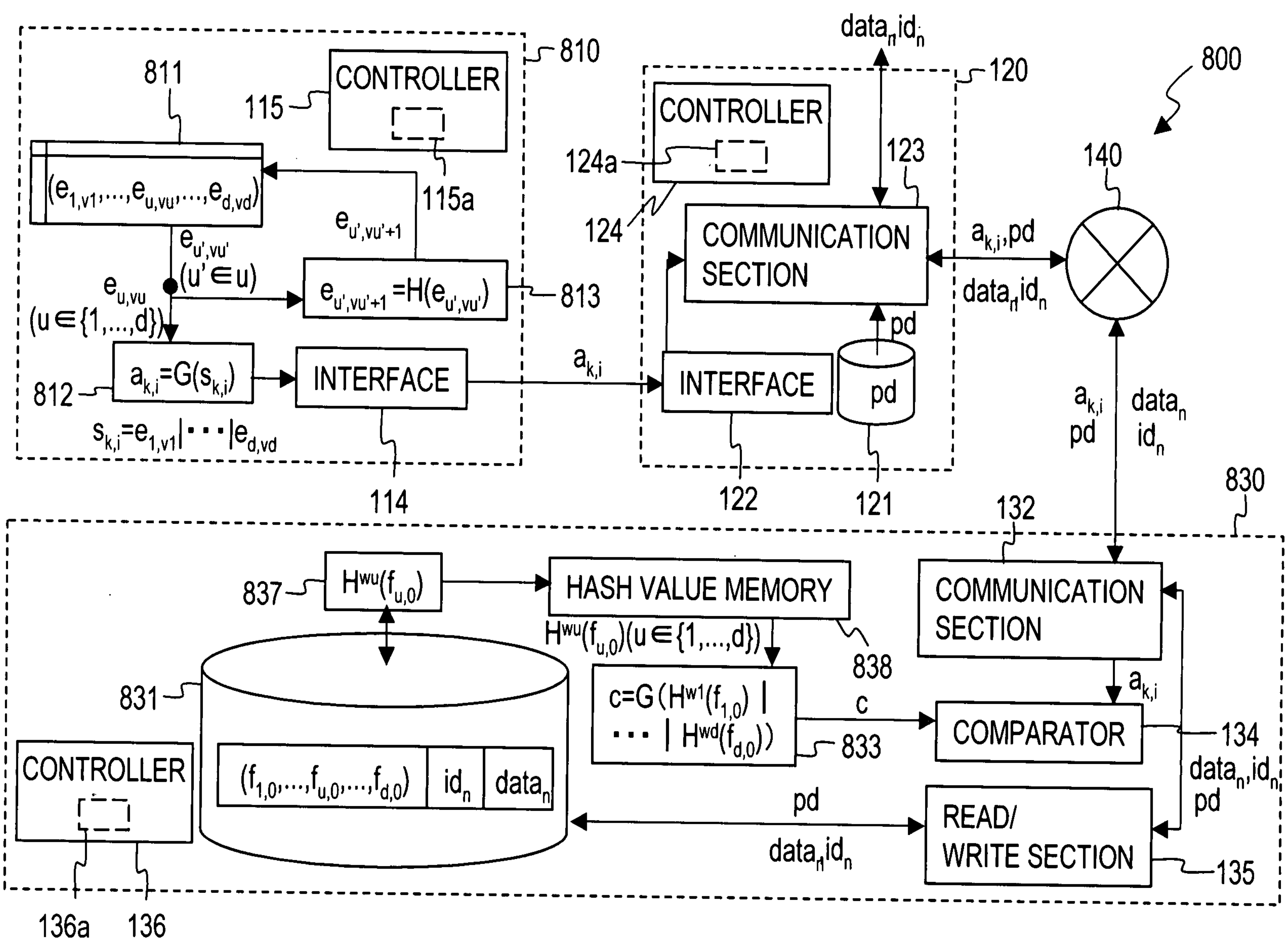

800
810
CONTROLLER
115
115a
811
$(e_{1,v1},\dots,e_{u,vu},\dots,e_{d,vd})$
$e_{u',vu'+1}$
$e_{u',vu'}$
$(u'\in u)$
$e_{u,vu}$
$(u\in\{1,\dots,d\})$
$e_{u',vu'+1}=H(e_{u',vu'})$
813
812
$a_{k,i}=G(s_{k,i})$
INTERFACE
$s_{k,i}=e_{1,v1}|\cdots|e_{d,vd}$
114
$a_{k,i}$
120
$data_n,id_n$
CONTROLLER
124a
124
123
COMMUNICATION SECTION
pd
INTERFACE
pd
122
121
$a_{k,i},pd$
$data_n,id_n$
140
$a_{k,i}$
pd
$data_n$
id_n
830
132
COMMUNICATION SECTION
837
$H^{wu}(f_{u,0})$
HASH VALUE MEMORY
$H^{wu}(f_{u,0})(u\in\{1,\dots,d\})$
838
831
$c=G(H^{w1}(f_{1,0})|\cdots|H^{wd}(f_{d,0}))$
c
833
$a_{k,i}$
COMPARATOR
134
$data_n,id_n$
pd
$(f_{1,0},\dots,f_{u,0},\dots,f_{d,0})$
id_n
$data_n$
CONTROLLER
136a
136
pd
$data_n,id_n$
READ/ WRITE SECTION
135

FIG.16

A

811a

$(e_{1,0},e_{2,0})$
$(b_{1,2,0},b_{2,2,0})$

B

831aa	831ab	831ac
$(f_{1,0},f_{2,0})$	id_n	$data_n$
$(b_{1,1,0},b_{2,1,0})$	id_1	$data_1$
$(b_{1,1,0},b_{2,2,0})$	id_2	$data_2$
$(b_{1,1,0},b_{2,3,0})$	id_3	$data_3$
$(b_{1,2,0},b_{2,1,0})$	id_4	$data_4$
$(b_{1,2,0},b_{2,2,0})$	id_5	$data_5$
$(b_{1,2,0},b_{2,3,0})$	id_6	$data_6$
$(b_{1,3,0},b_{2,1,0})$	id_7	$data_7$
$(b_{1,3,0},b_{2,2,0})$	id_8	$data_8$
$(b_{1,3,0},b_{2,3,0})$	id_9	$data_9$

$$f_{1,0} \in \{b_{1,1,0},b_{1,2,0},b_{1,3,0}\}$$
$$f_{2,0} \in \{b_{2,1,0},b_{2,2,0},b_{2,3,0}\}$$

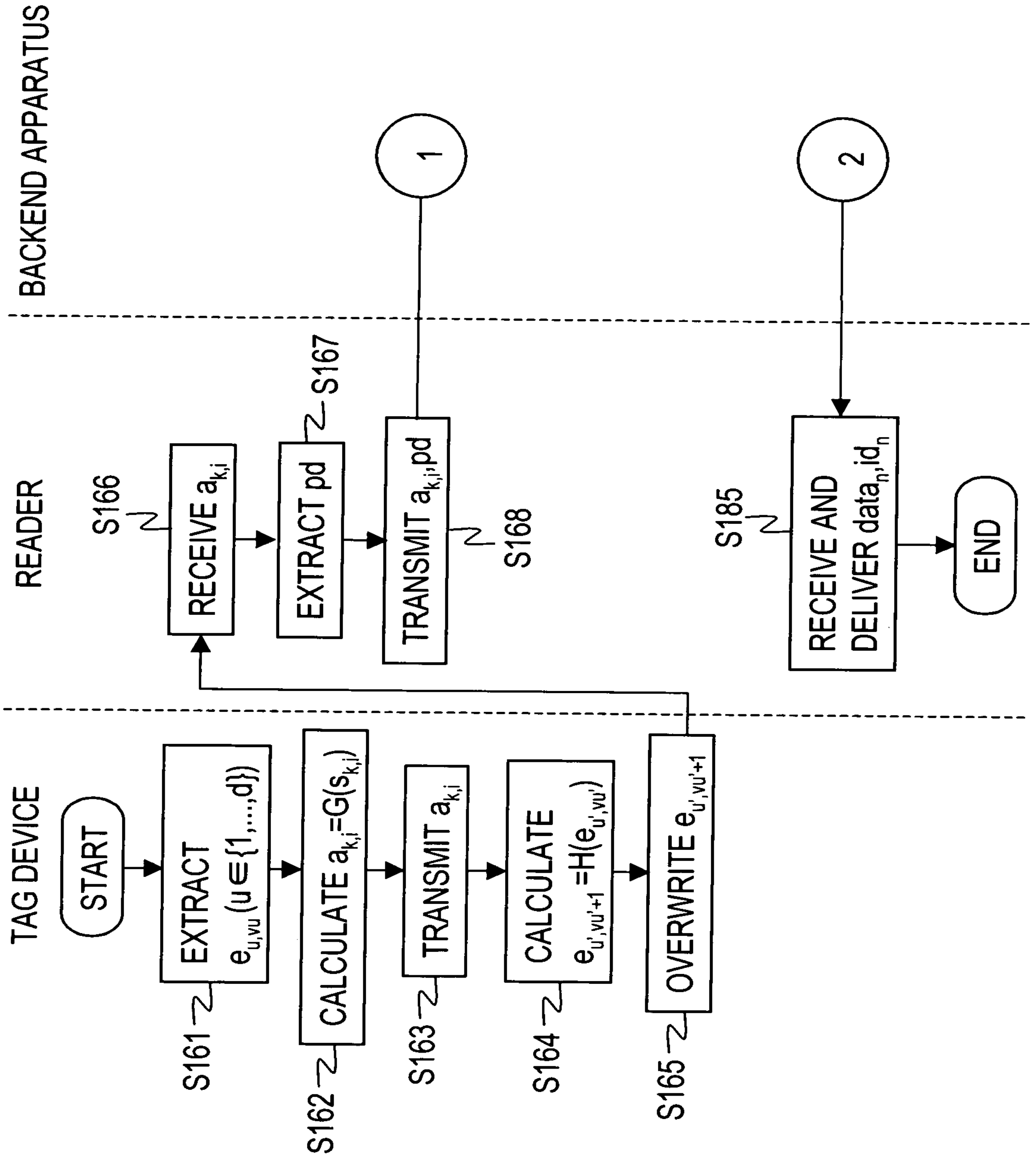

TAG DEVICE
READER
BACKEND APPARATUS
START
EXTRACT $e_{u,vu}$ ($u \in \{1,\ldots,d\}$)
S161
CALCULATE $a_{k,i}=G(s_{k,i})$
S162
TRANSMIT $a_{k,i}$
S163
CALCULATE $e_{u',vu'+1}=H(e_{u',vu'})$
S164
OVERWRITE $e_{u',vu'+1}$
S165
S166
RECEIVE $a_{k,i}$
EXTRACT pd
S167
TRANSMIT $a_{k,i}$,pd
S168
1
2
S185
RECEIVE AND DELIVER $data_n$,id_n
END

FIG.17

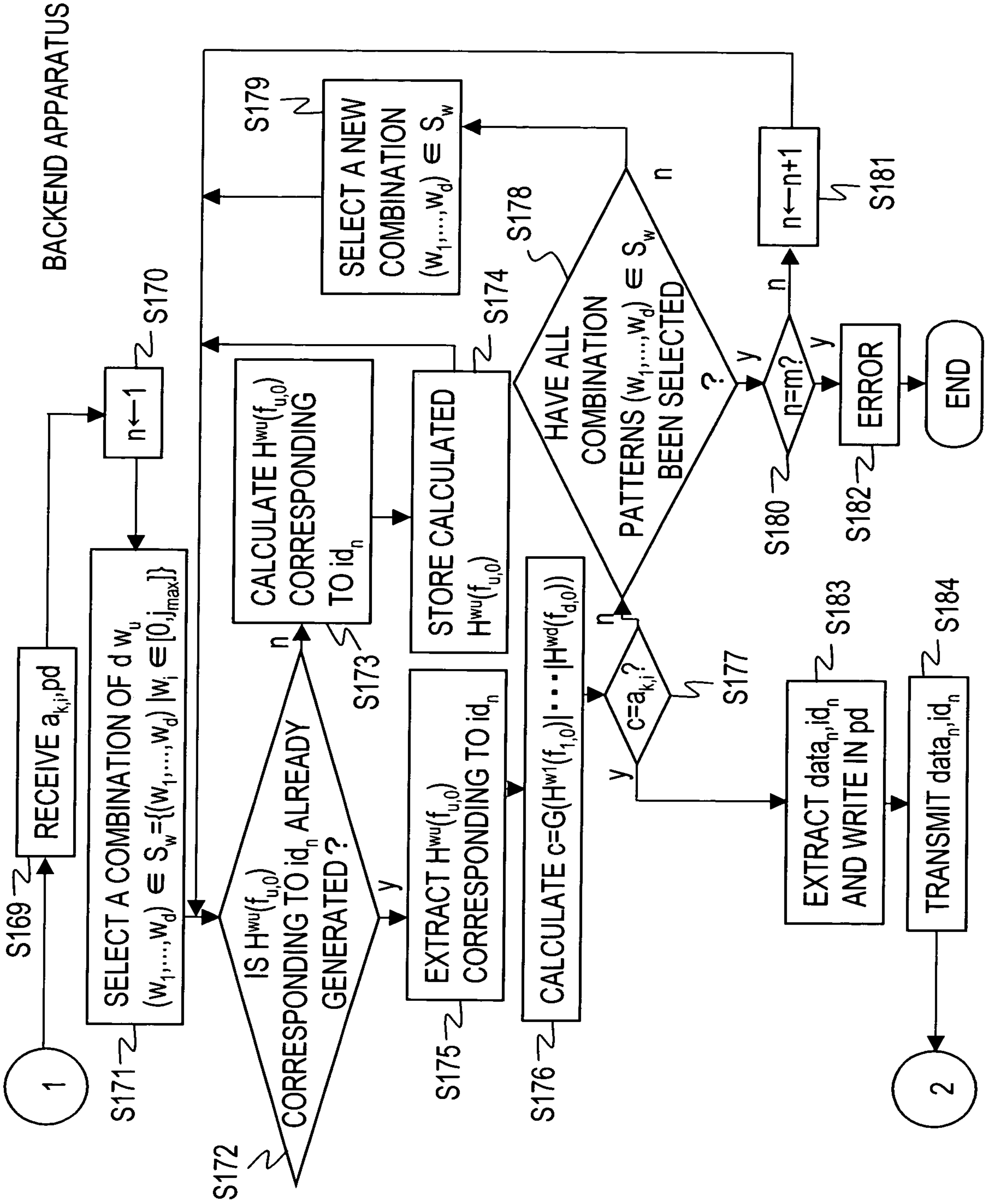

BACKEND APPARATUS
1
S169
RECEIVE $a_{k,i}$,pd
S170
$n \leftarrow 1$
S171
SELECT A COMBINATION OF d w_u $(w_1,\ldots,w_d) \in S_w=\{(w_1,\ldots,w_d)\,|w_i \in [0,j_{max}]\}$
S172
IS $H^{wu}(f_{u,0})$ CORRESPONDING TO id_n ALREADY GENERATED ?
y
n
S173
CALCULATE $H^{wu}(f_{u,0})$ CORRESPONDING TO id_n
S174
STORE CALCULATED $H^{wu}(f_{u,0})$
S175
EXTRACT $H^{wu}(f_{u,0})$ CORRESPONDING TO id_n
S176
CALCULATE $c=G(H^{w1}(f_{1,0})|\cdots|H^{wd}(f_{d,0}))$
S177
$c=a_{k,i}$?
y
n
S178
HAVE ALL COMBINATION PATTERNS $(w_1,\ldots,w_d) \in S_w$ BEEN SELECTED ?
y
n
S179
SELECT A NEW COMBINATION $(w_1,\ldots,w_d) \in S_w$
S180
n=m?
y
n
S181
$n \leftarrow n+1$
S182
ERROR
END
S183
EXTRACT $data_n$,id_n AND WRITE IN pd
S184
TRANSMIT $data_n$,id_n
2

FIG.18

FIG.19

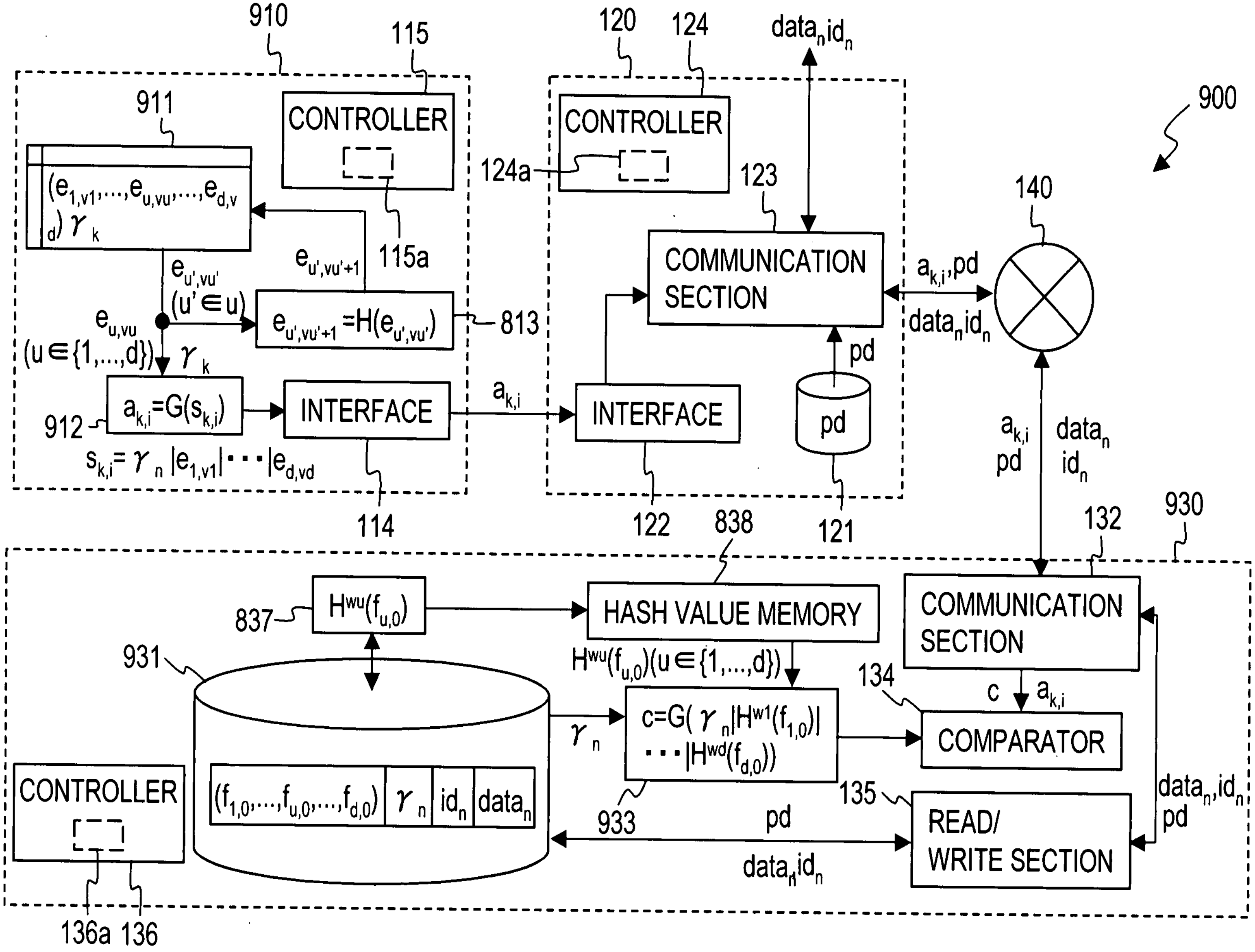

900
910
115
CONTROLLER
115a
911
$(e_{1,v1},\ldots,e_{u,vu},\ldots,e_{d,v_d})\gamma_k$
$e_{u',vu'+1}$
$e_{u',vu'}$
$(u'\in u)$
$e_{u',vu'+1}=H(e_{u',vu'})$
813
$e_{u,vu}$
$(u\in\{1,\ldots,d\})$
γ_k
912
$a_{k,i}=G(s_{k,i})$
INTERFACE
$s_{k,i}=\gamma_n|e_{1,v1}|\cdots|e_{d,vd}$
114
$a_{k,i}$
120
124
CONTROLLER
124a
123
COMMUNICATION SECTION
$data_n id_n$
INTERFACE
122
pd
pd
121
140
$a_{k,i}$,pd
$data_n id_n$
$a_{k,i}$
pd
$data_n$
id_n
930
132
COMMUNICATION SECTION
c
$a_{k,i}$
134
COMPARATOR
135
READ/ WRITE SECTION
$data_n,id_n$
pd
838
HASH VALUE MEMORY
837
$H^{wu}(f_{u,0})$
$H^{wu}(f_{u,0})(u\in\{1,\ldots,d\})$
$c=G(\gamma_n|H^{w1}(f_{1,0})|\cdots|H^{wd}(f_{d,0}))$
933
γ_n
931
$(f_{1,0},\ldots,f_{u,0},\ldots,f_{d,0})$
γ_n
id_n
$data_n$
pd
$data_n id_n$
CONTROLLER
136a
136

FIG.20

A

911a 911b

$(e_{1,0},e_{2,0})$	γ_k
$(b_{1,2,0},b_{2,2,0})$	γ_5

B

931aa 931ab 931ac 931ad

$(f_{1,0},f_{2,0})$	id_n	$data_n$	γ_k
$(b_{1,1,0},b_{2,1,0})$	id_1	$data_1$	γ_1
$(b_{1,1,0},b_{2,2,0})$	id_2	$data_2$	γ_2
$(b_{1,1,0},b_{2,3,0})$	id_3	$data_3$	γ_3
$(b_{1,2,0},b_{2,1,0})$	id_4	$data_4$	γ_4
$(b_{1,2,0},b_{2,2,0})$	id_5	$data_5$	γ_5
$(b_{1,2,0},b_{2,3,0})$	id_6	$data_6$	γ_6
$(b_{1,3,0},b_{2,1,0})$	id_7	$data_7$	γ_7
$(b_{1,3,0},b_{2,2,0})$	id_8	$data_8$	γ_8
$(b_{1,3,0},b_{2,3,0})$	id_9	$data_9$	γ_9

$f_{1,0} \in \{b_{1,1,0},b_{1,2,0},b_{1,3,0}\}$

$f_{2,0} \in \{b_{2,1,0},b_{2,2,0},b_{2,3,0}\}$

FIG.21

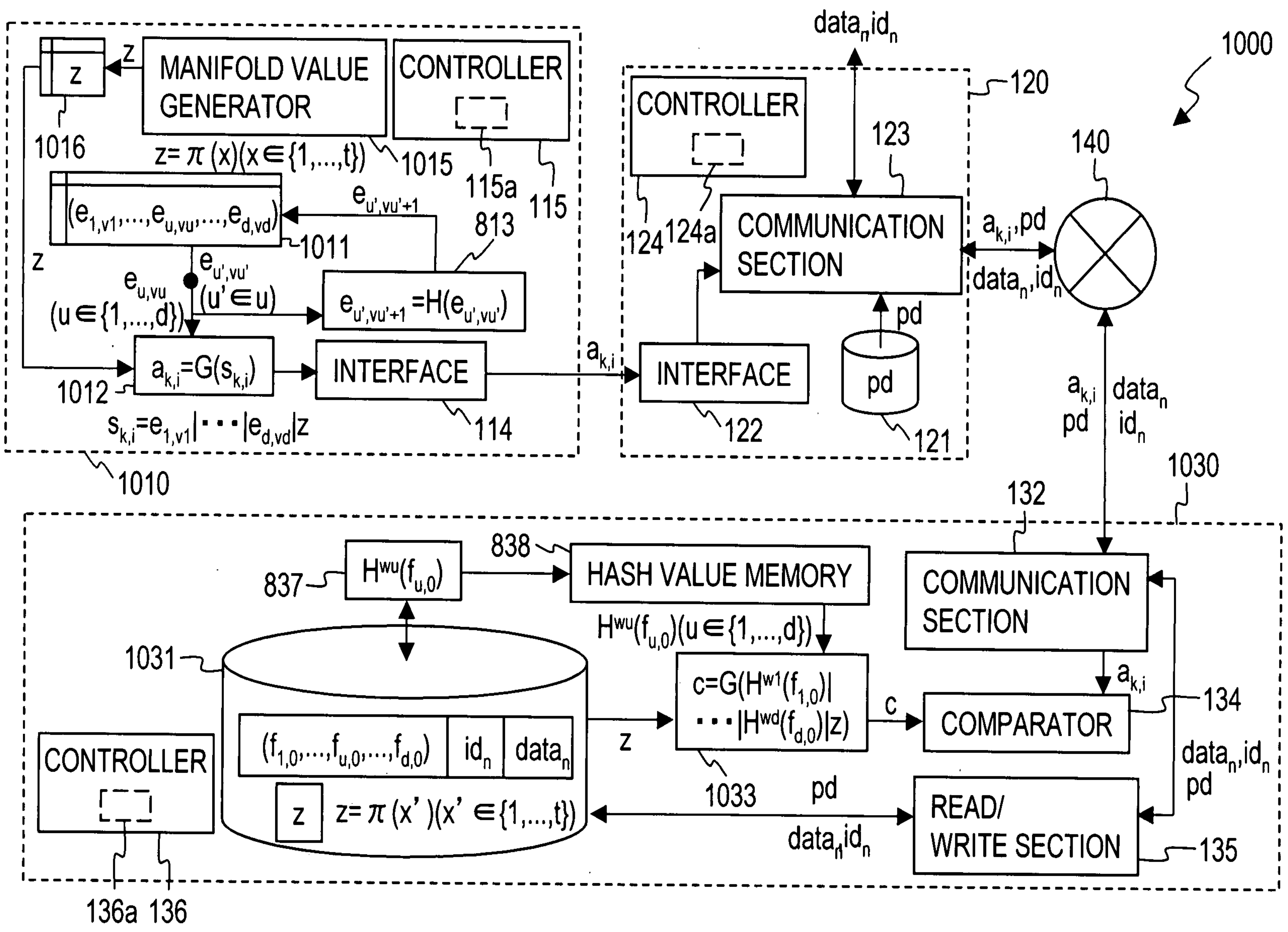
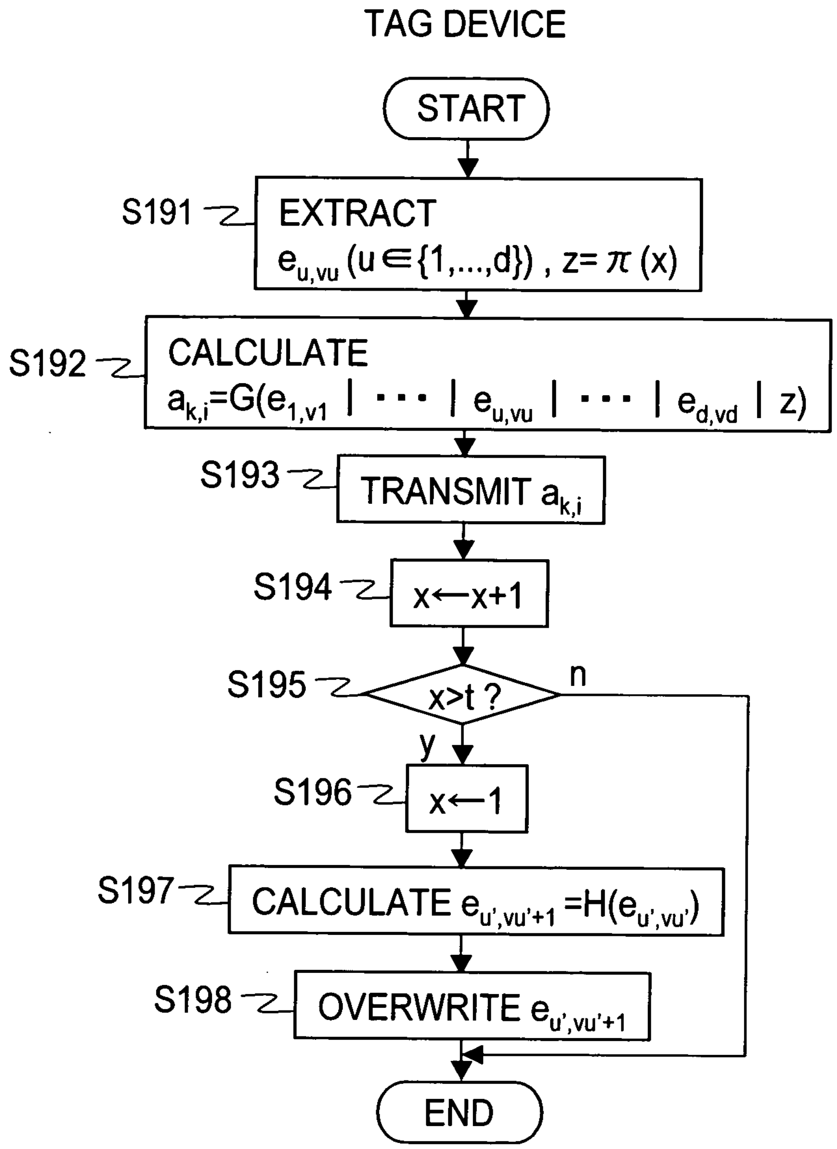

1000
1010
z
MANIFOLD VALUE GENERATOR
CONTROLLER
1016
$z=\pi(x)(x\in\{1,\ldots,t\})$
1015
115a
115
$(e_{1,v1},\ldots,e_{u,vu},\ldots,e_{d,vd})$
$e_{u',vu'+1}$
813
1011
z
$e_{u,vu}$
$(u\in\{1,\ldots,d\})$
$e_{u',vu'}$
$(u'\in u)$
$e_{u',vu'+1}=H(e_{u',vu'})$
$a_{k,i}=G(s_{k,i})$
INTERFACE
1012
$s_{k,i}=e_{1,v1}|\cdots|e_{d,vd}|z$
114
$a_{k,i}$
$data_n, id_n$
120
CONTROLLER
123
124
124a
COMMUNICATION SECTION
pd
INTERFACE
pd
122
121
140
$a_{k,i}$,pd
$data_n,id_n$
$a_{k,i}$
pd
$data_n$
id_n
1030
132
837
$H^{wu}(f_{u,0})$
838
HASH VALUE MEMORY
COMMUNICATION SECTION
1031
$H^{wu}(f_{u,0})(u\in\{1,\ldots,d\})$
$c=G(H^{w1}(f_{1,0})|\cdots|H^{wd}(f_{d,0})|z)$
$a_{k,i}$
c
COMPARATOR
134
$(f_{1,0},\ldots,f_{u,0},\ldots,f_{d,0})$
id_n
$data_n$
z
$data_n,id_n$
pd
CONTROLLER
z
$z=\pi(x')(x'\in\{1,\ldots,t\})$
1033
pd
$data_n,id_n$
READ/ WRITE SECTION
135
136a
136

FIG.22


TAG DEVICE
START
S191
EXTRACT
$e_{u,vu}$ ($u \in \{1,\ldots,d\}$) , $z=\pi(x)$
S192
CALCULATE
$a_{k,i}=G(e_{1,v1} \mid \cdots \mid e_{u,vu} \mid \cdots \mid e_{d,vd} \mid z)$
S193
TRANSMIT $a_{k,i}$
S194
$x \leftarrow x+1$
S195
$x>t$?
n
y
S196
$x \leftarrow 1$
S197
CALCULATE $e_{u',vu'+1}=H(e_{u',vu'})$
S198
OVERWRITE $e_{u',vu'+1}$
END

INITIAL VALUE x=1
UPON END, x VALUE MAINTAINED

FIG.23

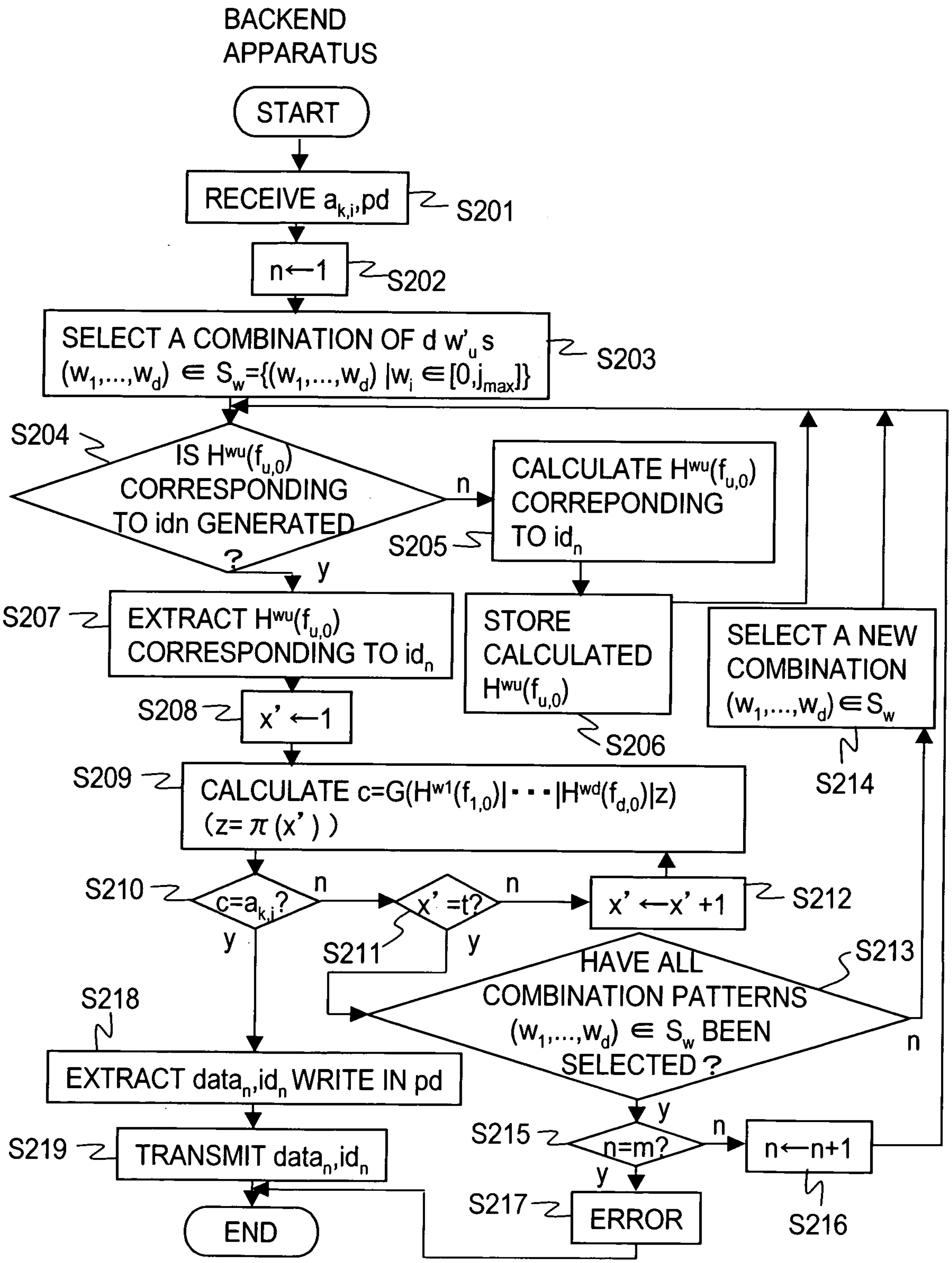

BACKEND APPARATUS
START
RECEIVE $a_{k,i}$,pd
S201
n←1
S202
SELECT A COMBINATION OF d w'$_u$ s
$(w_1,\ldots,w_d) \in S_w=\{(w_1,\ldots,w_d)\ |w_i \in [0,j_{max}]\}$
S203
S204
IS $H^{wu}(f_{u,0})$ CORRESPONDING TO idn GENERATED ?
n
y
CALCULATE $H^{wu}(f_{u,0})$ CORREPONDING TO id_n
S205
STORE CALCULATED $H^{wu}(f_{u,0})$
S206
SELECT A NEW COMBINATION $(w_1,\ldots,w_d) \in S_w$
S214
S207
EXTRACT $H^{wu}(f_{u,0})$ CORRESPONDING TO id_n
S208
x' ←1
S209
CALCULATE $c=G(H^{w1}(f_{1,0})|\cdots|H^{wd}(f_{d,0})|z)$ $(z=\pi(x'))$
S210
$c=a_{k,i}$?
n
y
S211
x' =t?
n
y
x' ←x' +1
S212
S213
HAVE ALL COMBINATION PATTERNS $(w_1,\ldots,w_d) \in S_w$ BEEN SELECTED ?
n
y
S218
EXTRACT $data_n$,id_n WRITE IN pd
S219
TRANSMIT $data_n$,id_n
END
S215
n=m?
n
y
n←n+1
S216
S217
ERROR

FIG.24

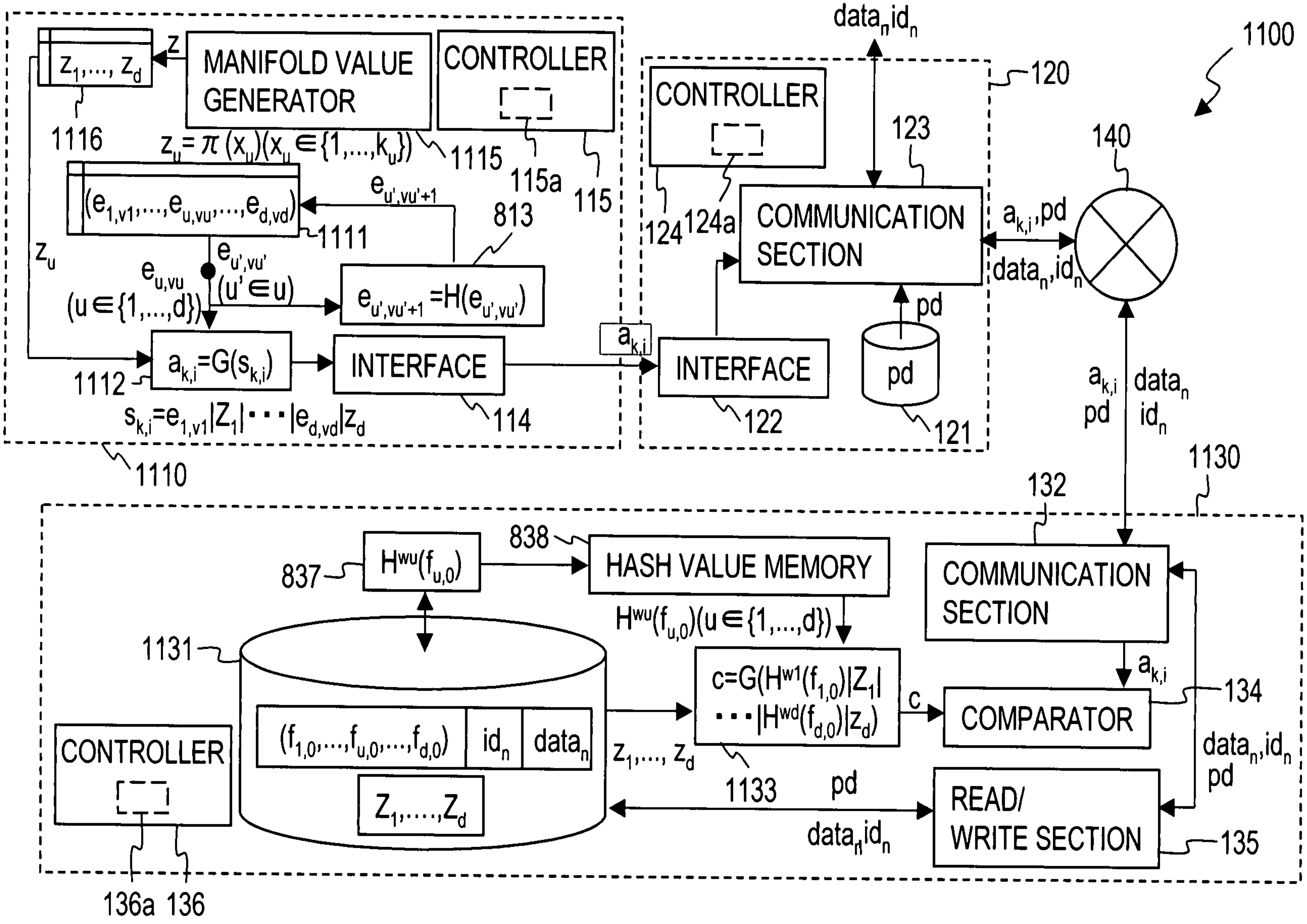
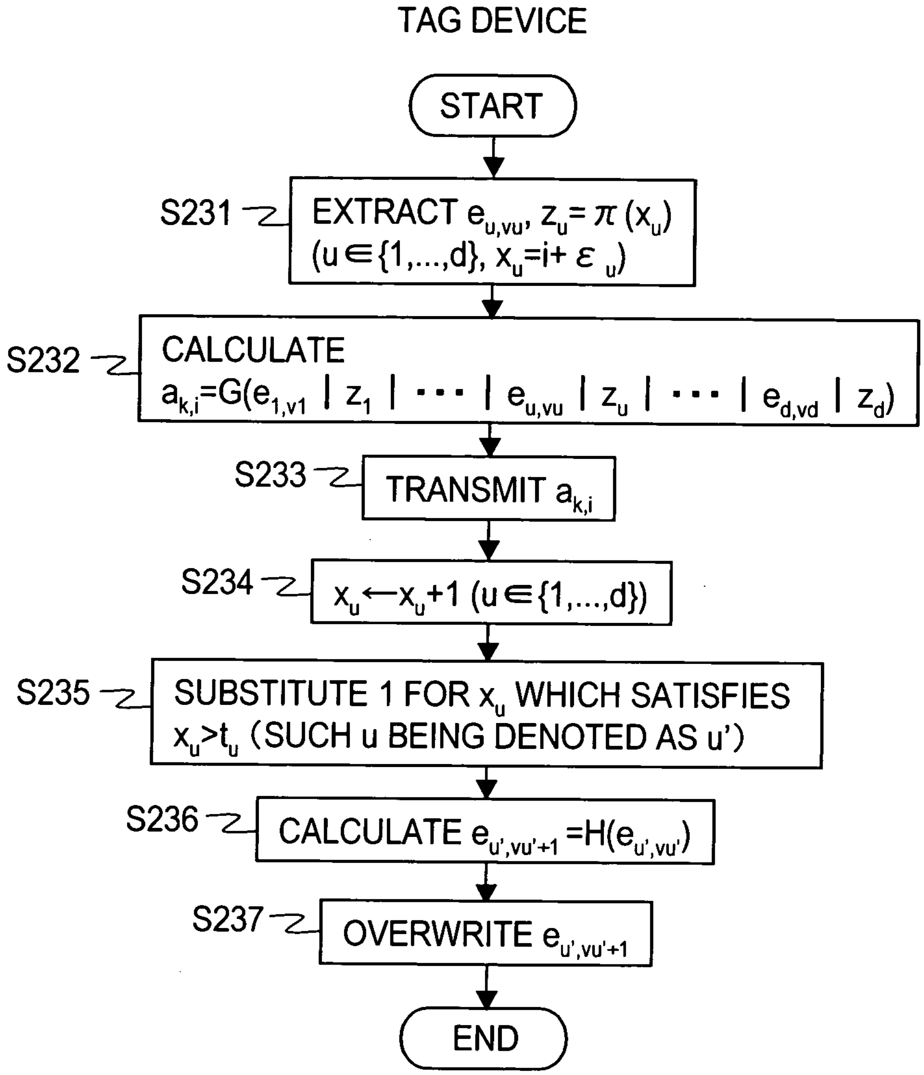

1100
1110
$z_1,\ldots,z_d$
1116
z
MANIFOLD VALUE GENERATOR
CONTROLLER
$z_u=\pi(x_u)(x_u\in\{1,\ldots,k_u\})$
1115
115a
115
$(e_{1,v1},\ldots,e_{u,vu},\ldots,e_{d,vd})$
1111
$e_{u',vu'+1}$
813
z_u
$e_{u,vu}$
$(u\in\{1,\ldots,d\})$
$e_{u',vu'}$
$(u'\in u)$
$e_{u',vu'+1}=H(e_{u',vu'})$
$a_{k,i}=G(s_{k,i})$
1112
INTERFACE
114
$s_{k,i}=e_{1,v1}|Z_1|\cdots|e_{d,vd}|z_d$
$a_{k,i}$
120
CONTROLLER
124
124a
$data_n,id_n$
123
COMMUNICATION SECTION
INTERFACE
122
pd
pd
121
$a_{k,i},pd$
$data_n,id_n$
140
$a_{k,i}$
pd
$data_n$
id_n
1130
132
COMMUNICATION SECTION
$a_{k,i}$
134
COMPARATOR
$data_n,id_n$
pd
READ/ WRITE SECTION
135
837
$H^{wu}(f_{u,0})$
838
HASH VALUE MEMORY
$H^{wu}(f_{u,0})(u\in\{1,\ldots,d\})$
$c=G(H^{w1}(f_{1,0})|Z_1|\cdots|H^{wd}(f_{d,0})|z_d)$
c
1133
1131
$(f_{1,0},\ldots,f_{u,0},\ldots,f_{d,0})$
id_n
$data_n$
$Z_1,\ldots,Z_d$
$z_1,\ldots,z_d$
pd
$data_n,id_n$
CONTROLLER
136a
136

FIG.25


TAG DEVICE
START
S231
EXTRACT $e_{u,vu}$, $z_u = \pi(x_u)$ ($u \in \{1,\dots,d\}$, $x_u = i + \varepsilon_u$)
S232
CALCULATE $a_{k,i} = G(e_{1,v1} \mid z_1 \mid \cdots \mid e_{u,vu} \mid z_u \mid \cdots \mid e_{d,vd} \mid z_d)$
S233
TRANSMIT $a_{k,i}$
S234
$x_u \leftarrow x_u + 1$ ($u \in \{1,\dots,d\}$)
S235
SUBSTITUTE 1 FOR x_u WHICH SATISFIES $x_u > t_u$ (SUCH u BEING DENOTED AS u')
S236
CALCULATE $e_{u',vu'+1} = H(e_{u',vu'})$
S237
OVERWRITE $e_{u',vu'+1}$
END

INITIAL VALUE OF $x_u = 1 + \varepsilon_u (u \in \{1,\dots,d\})$
UPON END , x VALUE MAINTAINED

FIG.26

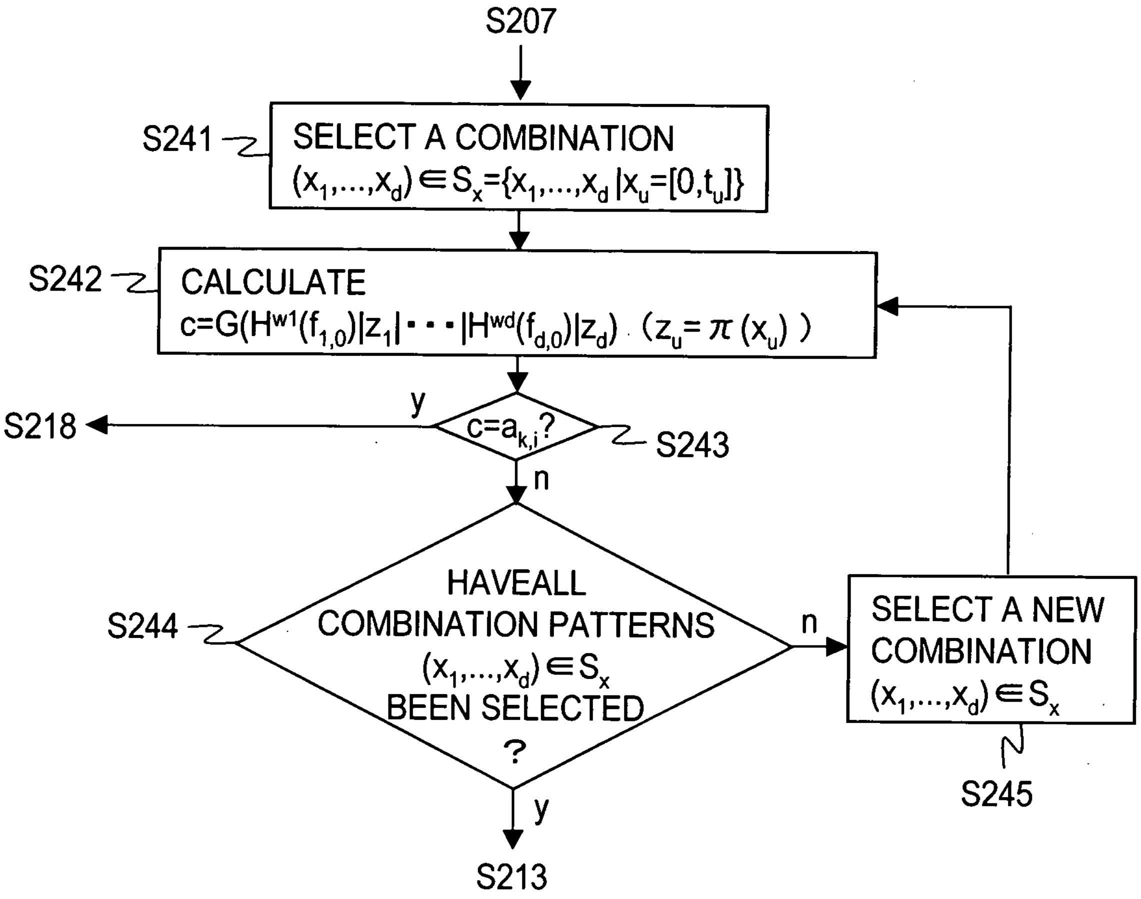
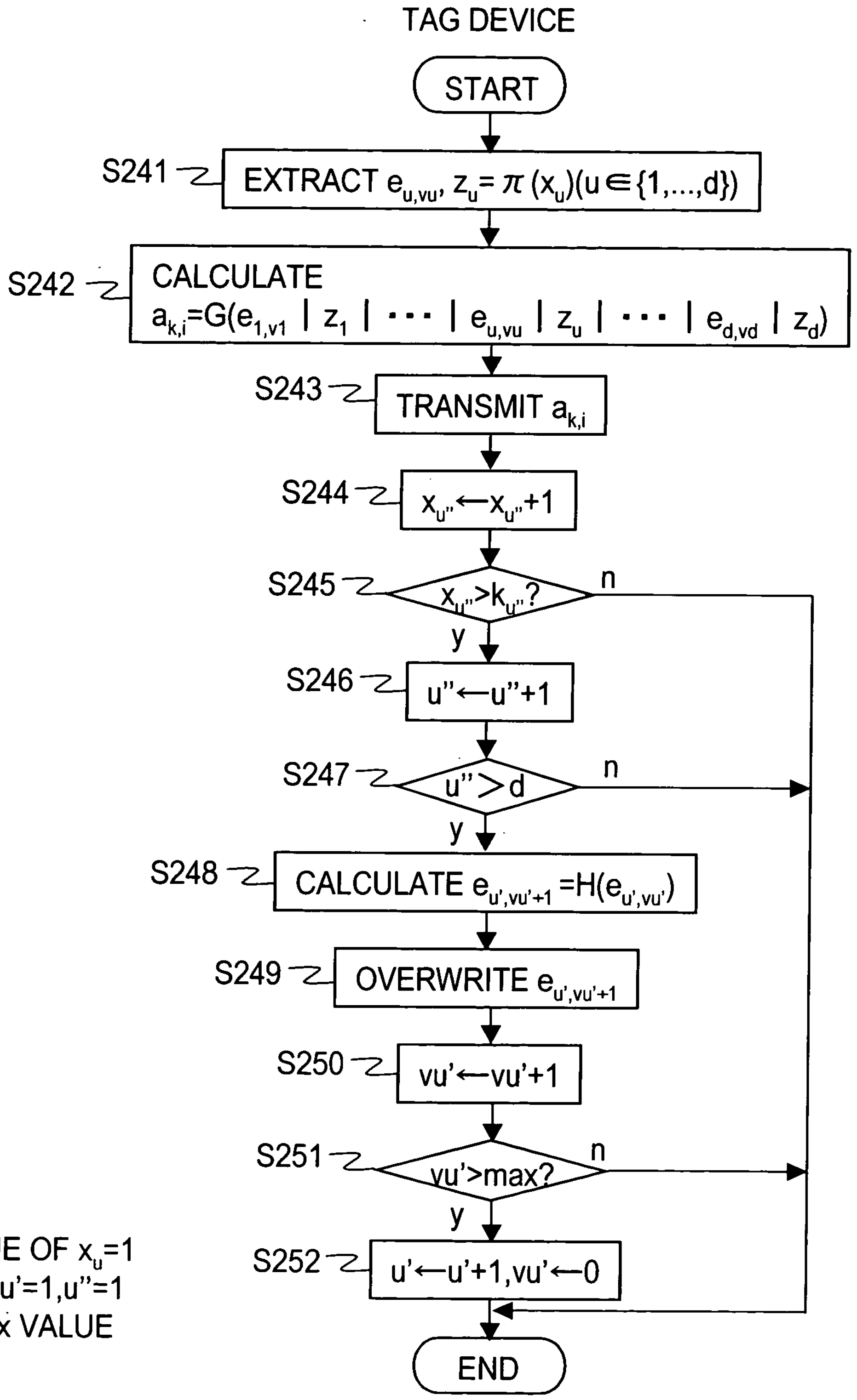

S207
S241
SELECT A COMBINATION $(x_1,\ldots,x_d)\in S_x=\{x_1,\ldots,x_d\,|x_u=[0,t_u]\}$
S242
CALCULATE $c=G(H^{w1}(f_{1,0})|z_1|\cdots|H^{wd}(f_{d,0})|z_d)$ $(z_u=\pi(x_u))$
y
S218
$c=a_{k,i}$?
S243
n
S244
HAVEALL COMBINATION PATTERNS $(x_1,\ldots,x_d)\in S_x$ BEEN SELECTED ?
n
SELECT A NEW COMBINATION $(x_1,\ldots,x_d)\in S_x$
S245
y
S213

FIG.27


TAG DEVICE
START
S241
EXTRACT $e_{u,vu}$, $z_u = \pi(x_u)(u \in \{1,...,d\})$
S242
CALCULATE
$a_{k,i}=G(e_{1,v1} \mid z_1 \mid \cdots \mid e_{u,vu} \mid z_u \mid \cdots \mid e_{d,vd} \mid z_d)$
S243
TRANSMIT $a_{k,i}$
S244
$x_{u''} \leftarrow x_{u''}+1$
S245
$x_{u''}>k_{u''}$?
n
y
S246
u"←u"+1
S247
u">d
n
y
S248
CALCULATE $e_{u',vu'+1}=H(e_{u',vu'})$
S249
OVERWRITE $e_{u',vu'+1}$
S250
vu'←vu'+1
S251
vu'>max?
n
y
S252
u'←u'+1,vu'←0
END

INITIAL VALUE OF $x_u=1$
$(u \in \{1,...,d\})$,u'=1,u"=1
UPON END , x VALUE
MAINTAINED

FIG.28

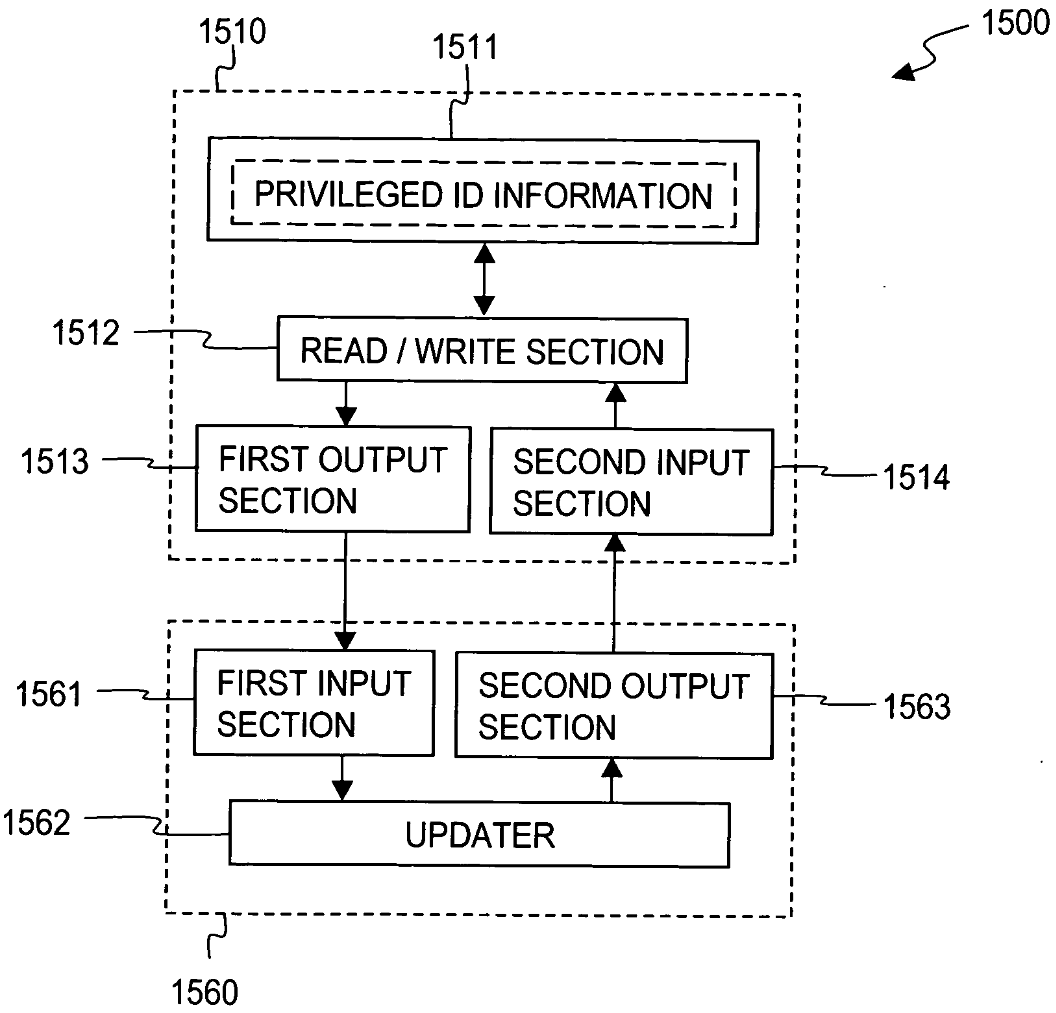

1500
1510
1511
PRIVILEGED ID INFORMATION
1512
READ / WRITE SECTION
1513
FIRST OUTPUT SECTION
SECOND INPUT SECTION
1514
1561
FIRST INPUT SECTION
SECOND OUTPUT SECTION
1563
1562
UPDATER
1560

FIG.29

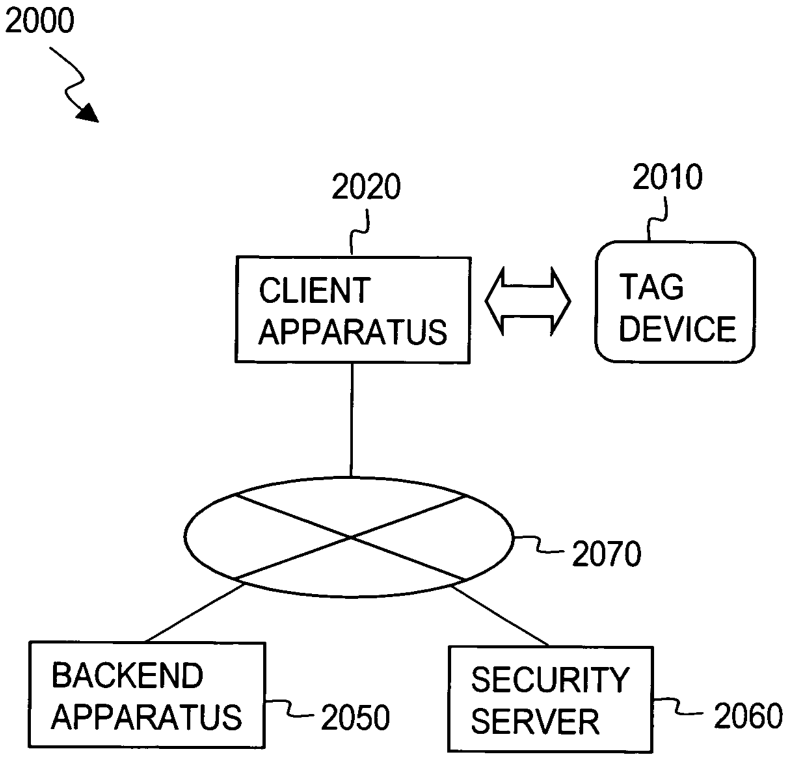

2000
2020
CLIENT APPARATUS
2010
TAG DEVICE
2070
BACKEND APPARATUS
2050
SECURITY SERVER
2060

FIG.30

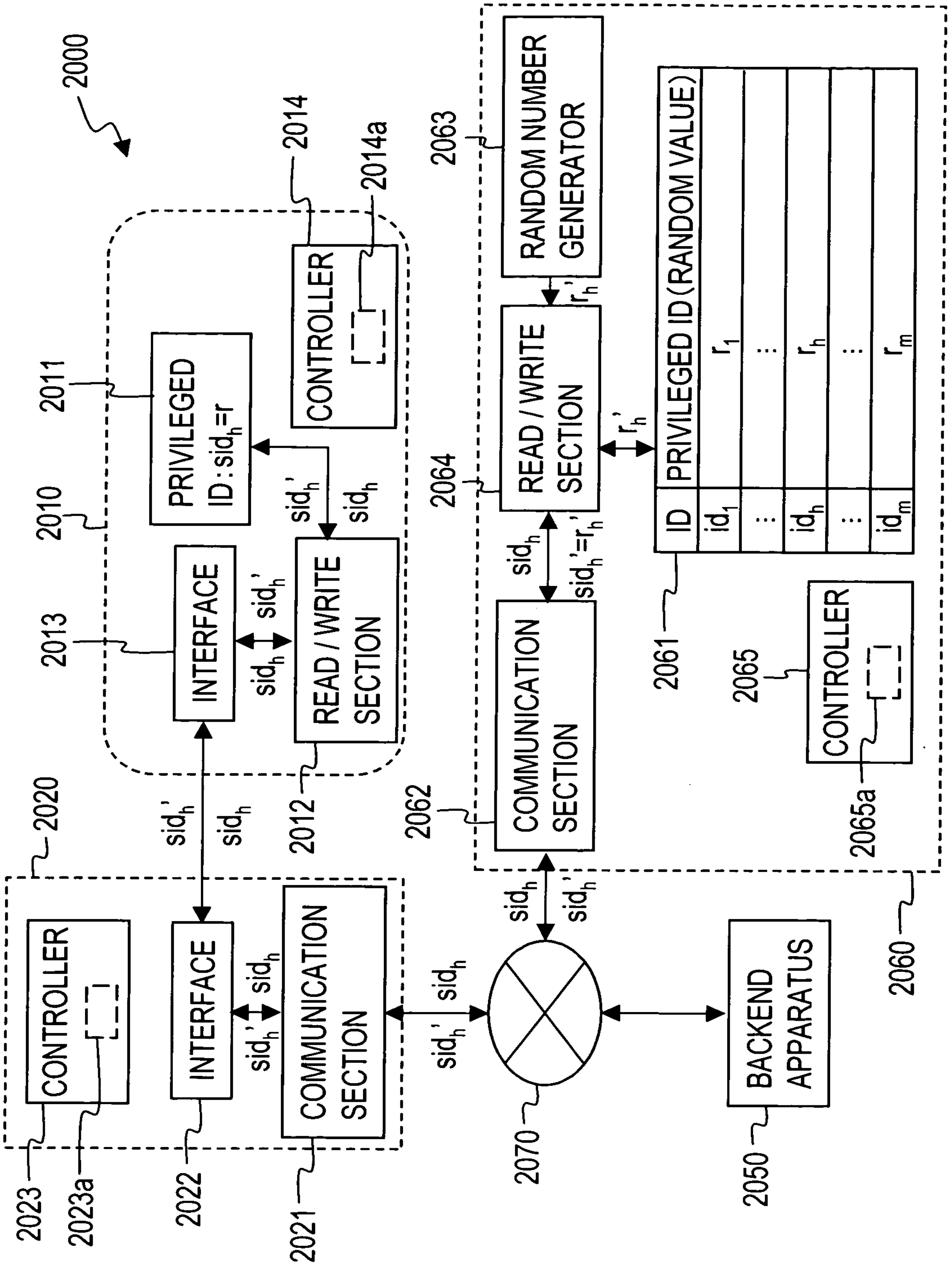

2000
2010
2011
PRIVILEGED ID: sid_h=r
2013
INTERFACE
sid_h
sid_h'
READ / WRITE SECTION
2012
2014
CONTROLLER
2014a
2020
CONTROLLER
2023
2023a
INTERFACE
2022
COMMUNICATION SECTION
2021
2070
BACKEND APPARATUS
2050
2060
COMMUNICATION SECTION
2062
READ / WRITE SECTION
2064
RANDOM NUMBER GENERATOR
2063
r_h'
sid_h'=r_h'
ID
PRIVILEGED ID (RANDOM VALUE)
id_1
r_1
...
id_h
r_h
id_m
r_m
2061
CONTROLLER
2065
2065a

FIG.31

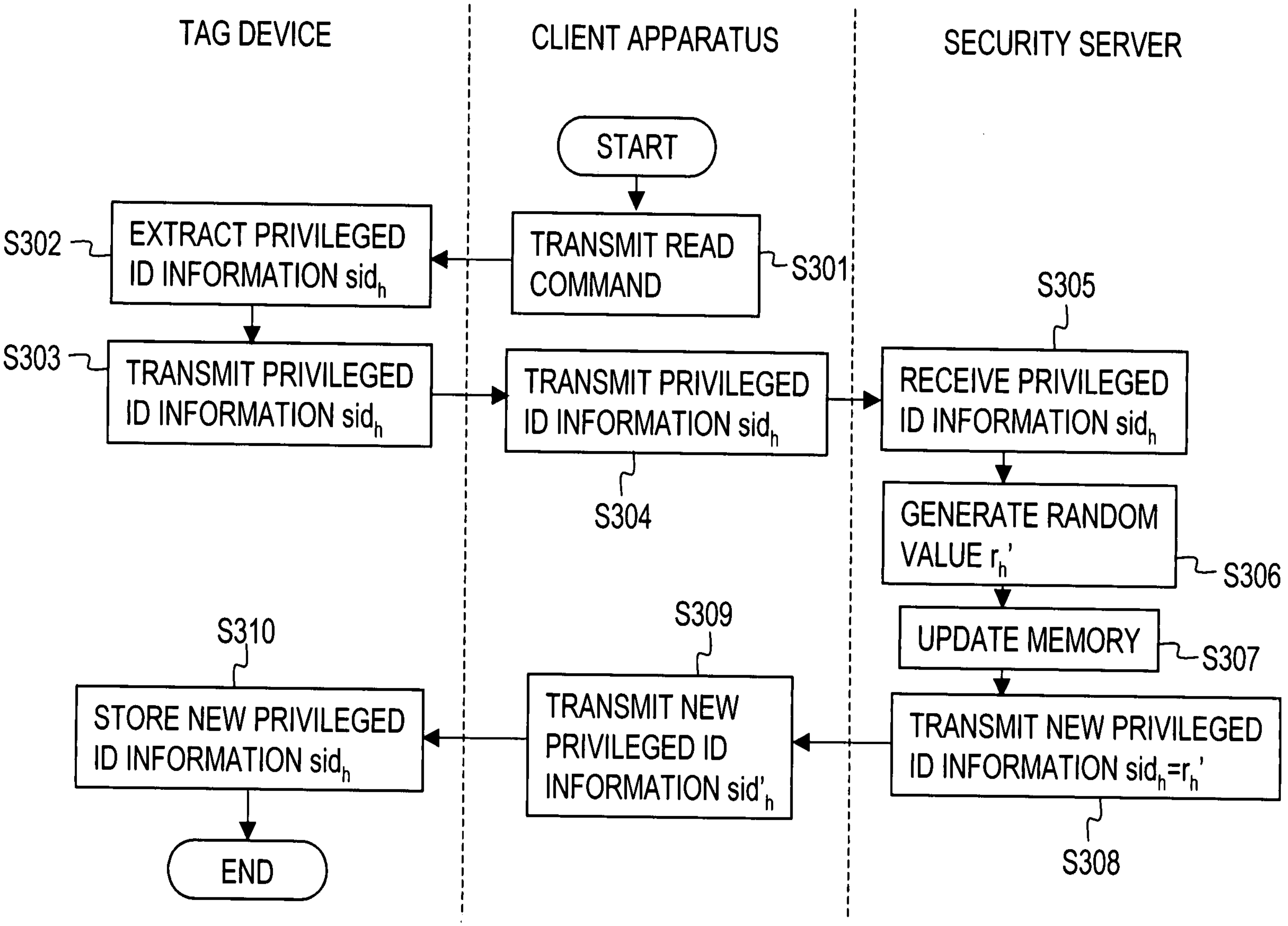
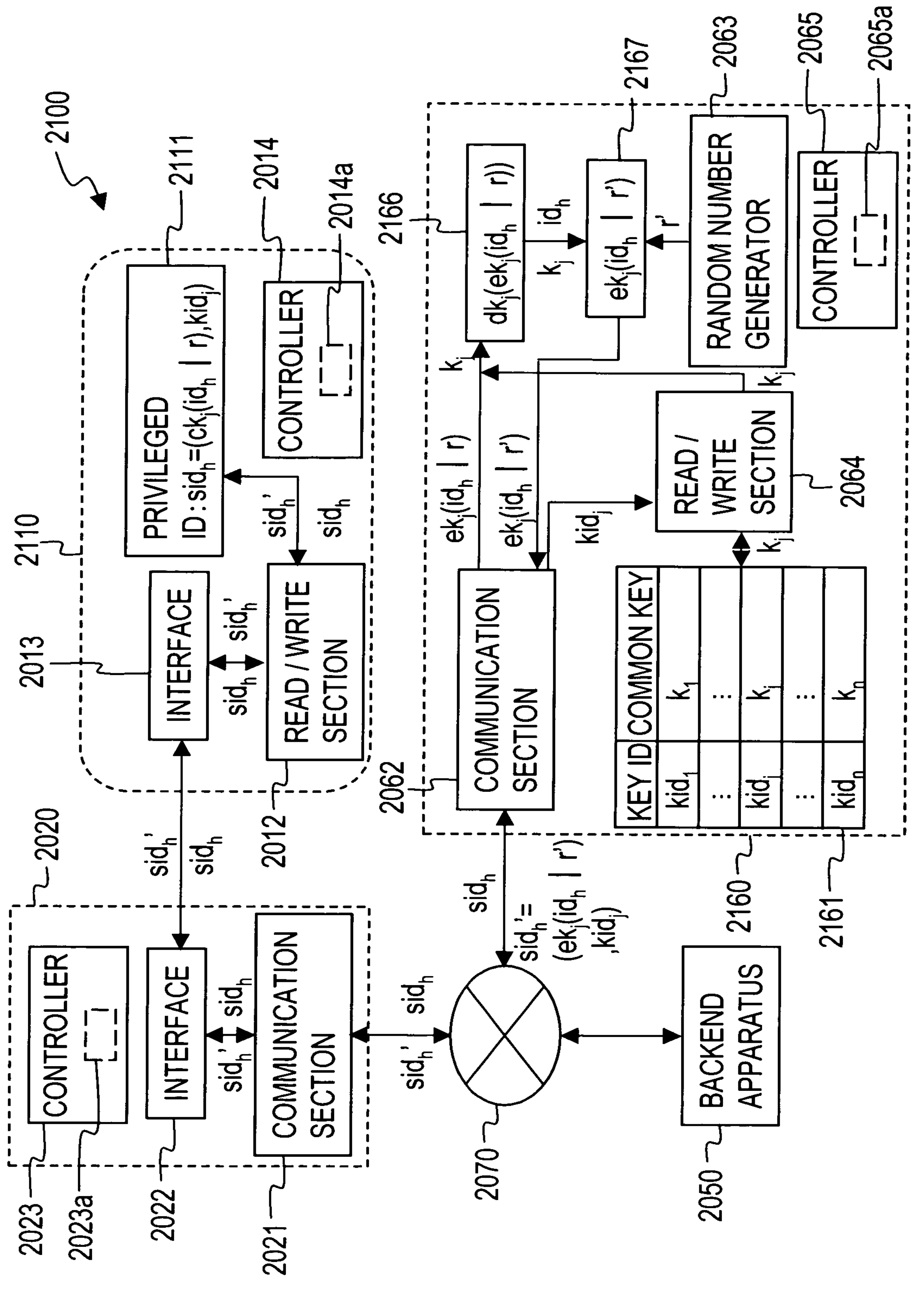

TAG DEVICE
CLIENT APPARATUS
SECURITY SERVER
START
TRANSMIT READ COMMAND
S301
EXTRACT PRIVILEGED ID INFORMATION sid_h
S302
TRANSMIT PRIVILEGED ID INFORMATION sid_h
S303
TRANSMIT PRIVILEGED ID INFORMATION sid_h
S304
S305
RECEIVE PRIVILEGED ID INFORMATION sid_h
GENERATE RANDOM VALUE r_h'
S306
UPDATE MEMORY
S307
TRANSMIT NEW PRIVILEGED ID INFORMATION $sid_h=r_h'$
S308
S309
TRANSMIT NEW PRIVILEGED ID INFORMATION sid'_h
S310
STORE NEW PRIVILEGED ID INFORMATION sid_h
END

FIG.32



KEY ID	COMMON KEY
kid_1	k_1
⋮	⋮
kid_j	k_j
⋮	⋮
kid_n	k_n

FIG.33

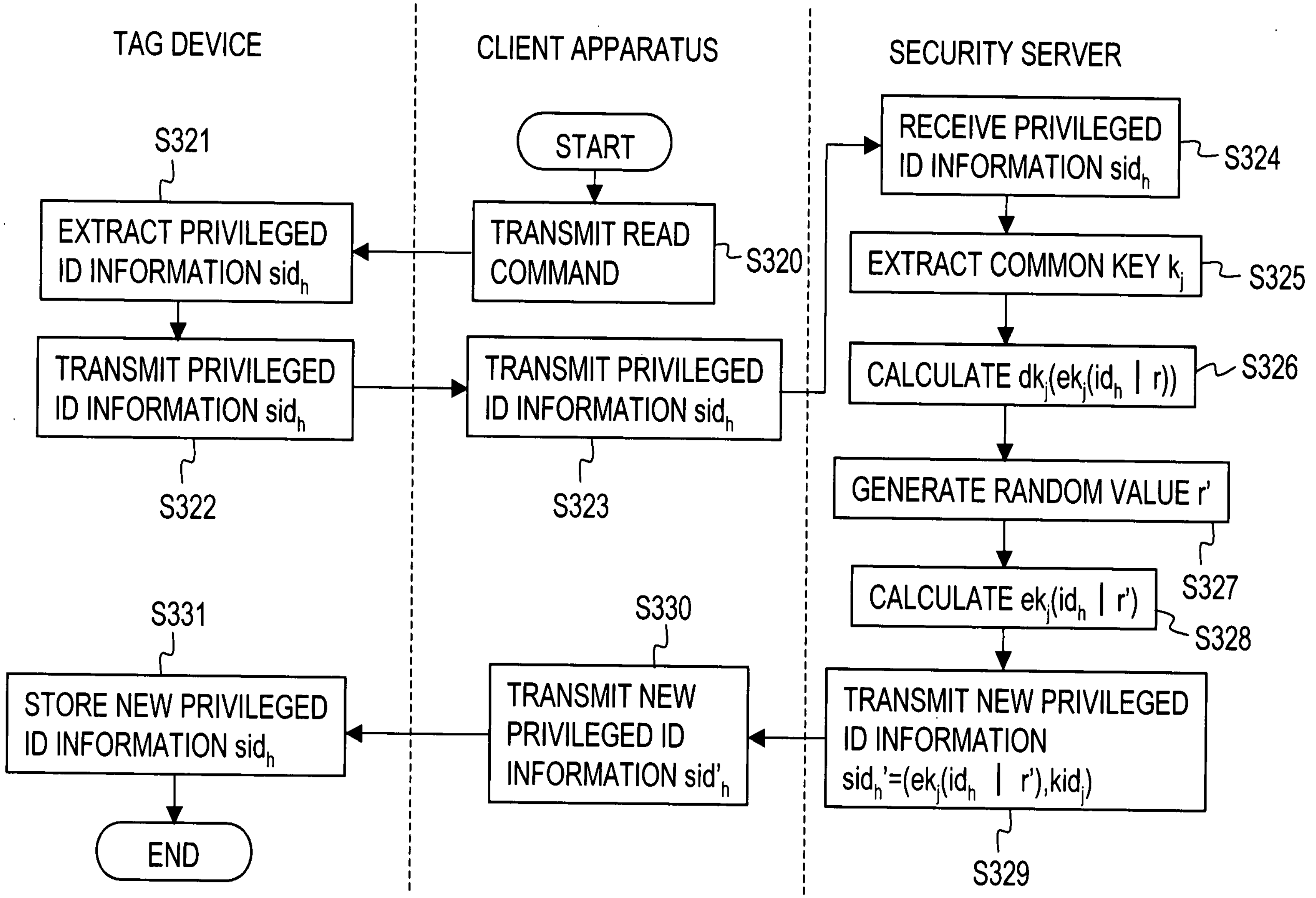
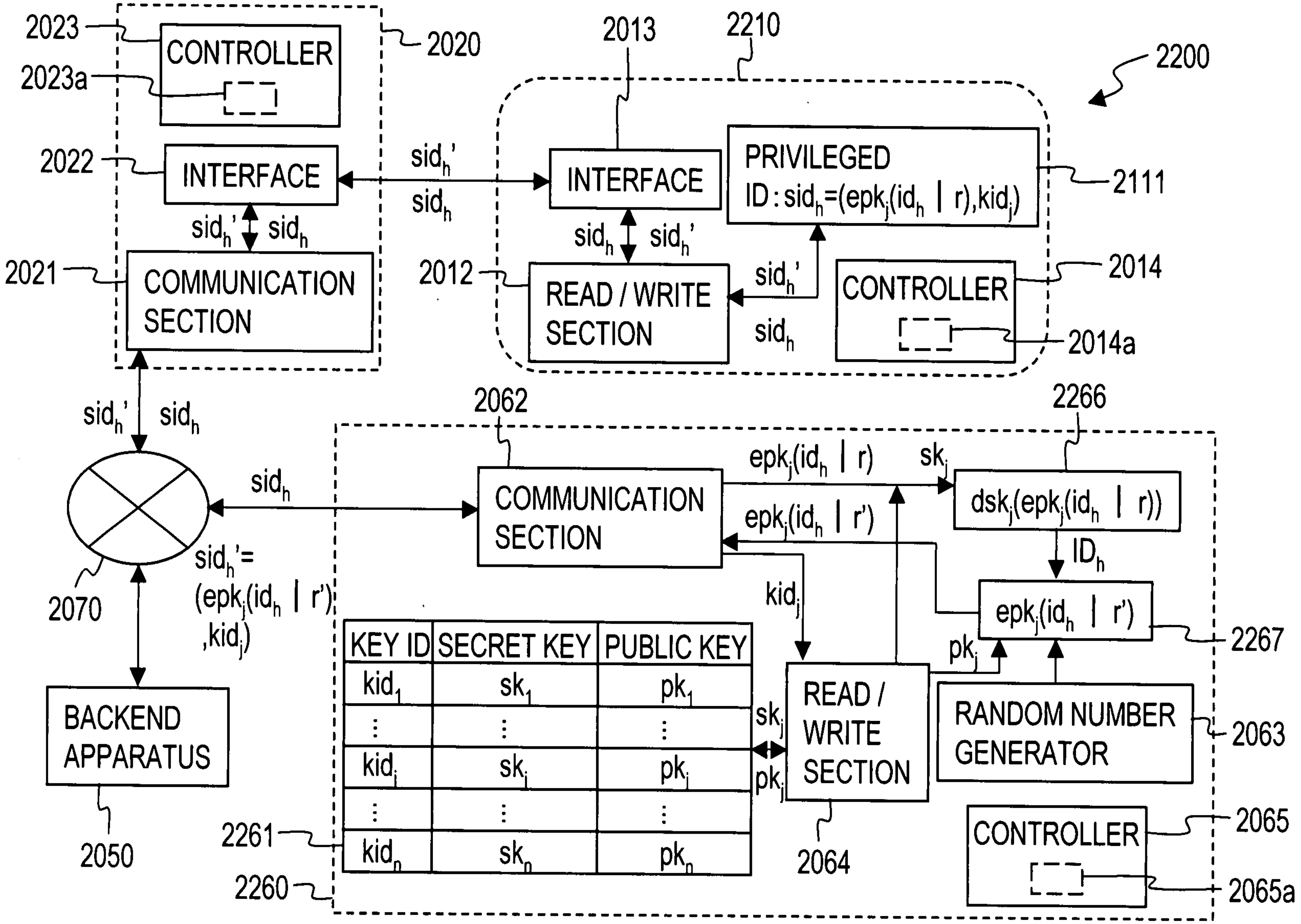

TAG DEVICE
CLIENT APPARATUS
SECURITY SERVER
START
TRANSMIT READ COMMAND
S320
S321
EXTRACT PRIVILEGED ID INFORMATION sid_h
TRANSMIT PRIVILEGED ID INFORMATION sid_h
S322
TRANSMIT PRIVILEGED ID INFORMATION sid_h
S323
RECEIVE PRIVILEGED ID INFORMATION sid_h
S324
EXTRACT COMMON KEY k_j
S325
CALCULATE $dk_j(ek_j(id_h \mid r))$
S326
GENERATE RANDOM VALUE r'
S327
CALCULATE $ek_j(id_h \mid r')$
S328
TRANSMIT NEW PRIVILEGED ID INFORMATION $sid_h'=(ek_j(id_h \mid r'),kid_j)$
S329
S330
TRANSMIT NEW PRIVILEGED ID INFORMATION sid'_h
S331
STORE NEW PRIVILEGED ID INFORMATION sid_h
END

FIG.34



KEY ID	SECRET KEY	PUBLIC KEY
kid_1	sk_1	pk_1
⋮	⋮	⋮
kid_j	sk_j	pk_j
⋮	⋮	⋮
kid_n	sk_n	pk_n

FIG.35

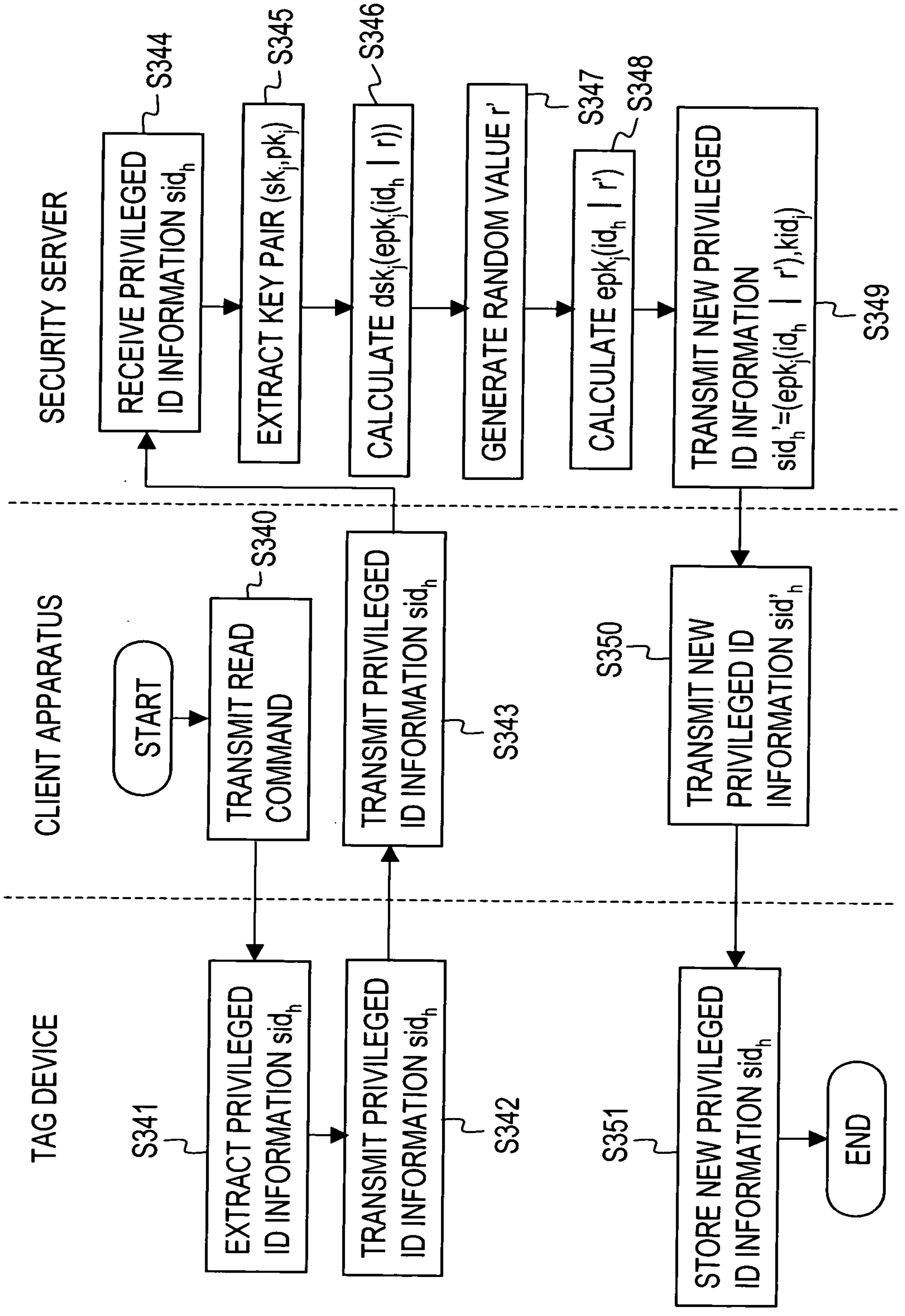
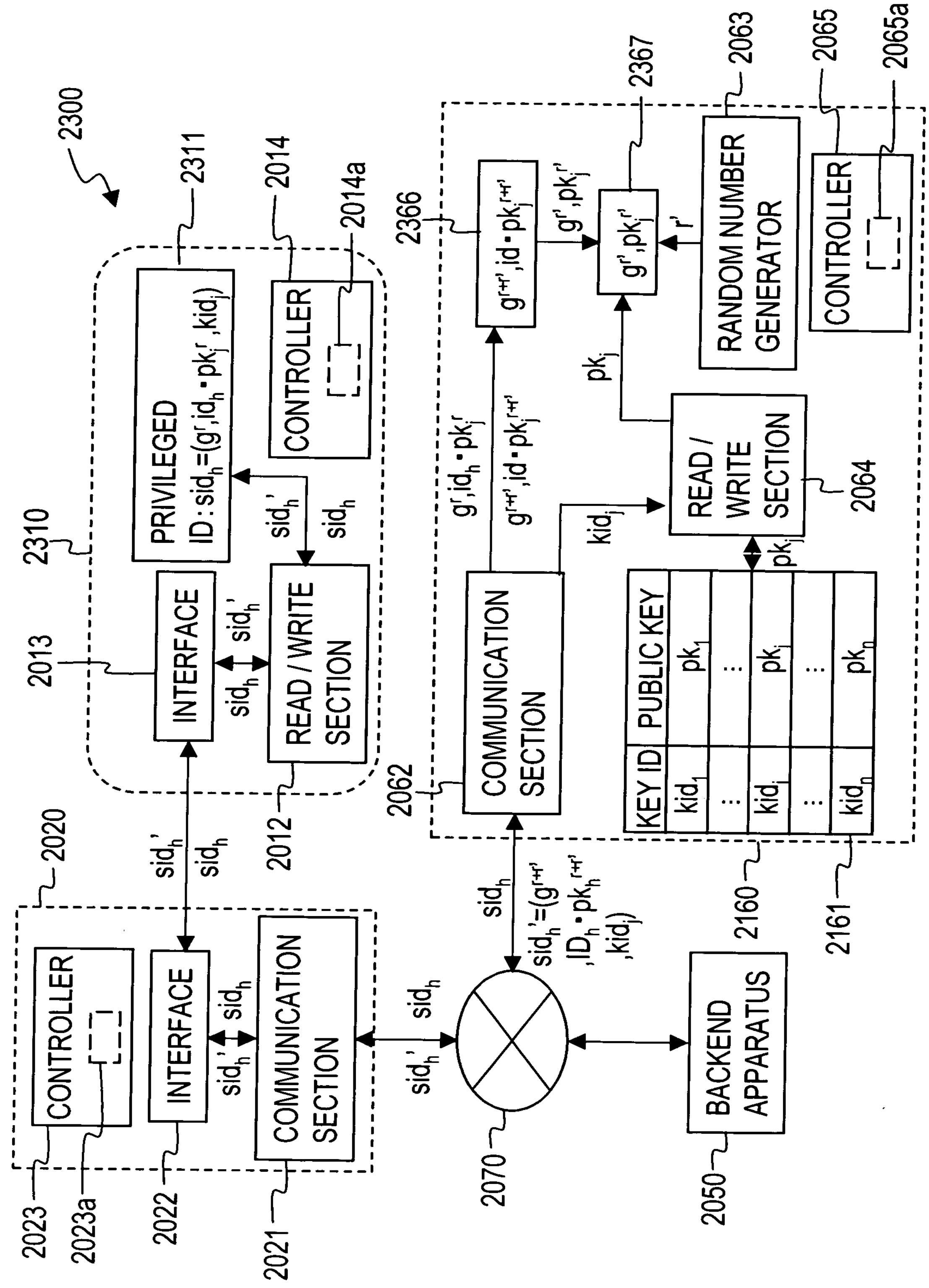

TAG DEVICE
CLIENT APPARATUS
SECURITY SERVER
START
TRANSMIT READ COMMAND
S340
S341
EXTRACT PRIVILEGED ID INFORMATION sid_h
S342
TRANSMIT PRIVILEGED ID INFORMATION sid_h
S343
TRANSMIT PRIVILEGED ID INFORMATION sid_h
S344
RECEIVE PRIVILEGED ID INFORMATION sid_h
S345
EXTRACT KEY PAIR (sk_j,pk_j)
S346
CALCULATE $dsk_j(epk_j(id_h \| r))$
S347
GENERATE RANDOM VALUE r'
S348
CALCULATE $epk_j(id_h \| r')$
S349
TRANSMIT NEW PRIVILEGED ID INFORMATION $sid_h'=(epk_j(id_h \| r'),kid_j)$
S350
TRANSMIT NEW PRIVILEGED ID INFORMATION sid_h'
S351
STORE NEW PRIVILEGED ID INFORMATION sid_h
END

FIG.36


2300
2310
2311
PRIVILEGED ID : $sid_h=(g^r, id_h \bullet pk_j^r, kid_j)$
2014
CONTROLLER
2014a
2013
INTERFACE
sid_h
sid_h'
2012
READ / WRITE SECTION
2020
2023
CONTROLLER
2023a
2022
INTERFACE
2021
COMMUNICATION SECTION
2070
2050
BACKEND APPARATUS
$sid_h'=(g^{r+r'}, ID_h \bullet pk_j^{r+r'}, kid_j)$
2062
COMMUNICATION SECTION
$g^r, id_h \bullet pk_j^r$
$g^{r+r'}, id \bullet pk_j^{r+r'}$
kid_j
2366
$g^{r+r'}, id \bullet pk_j^{r+r'}$
$g^{r'}, pk_j^{r'}$
2367
$g^{r'}, pk_j^{r'}$
r'
pk_j
2064
READ / WRITE SECTION
pk_j
2063
RANDOM NUMBER GENERATOR
2065
2065a
CONTROLLER
2160
2161
KEY ID
PUBLIC KEY
kid_1
pk_1
...
kid_j
pk_j
kid_n
pk_n

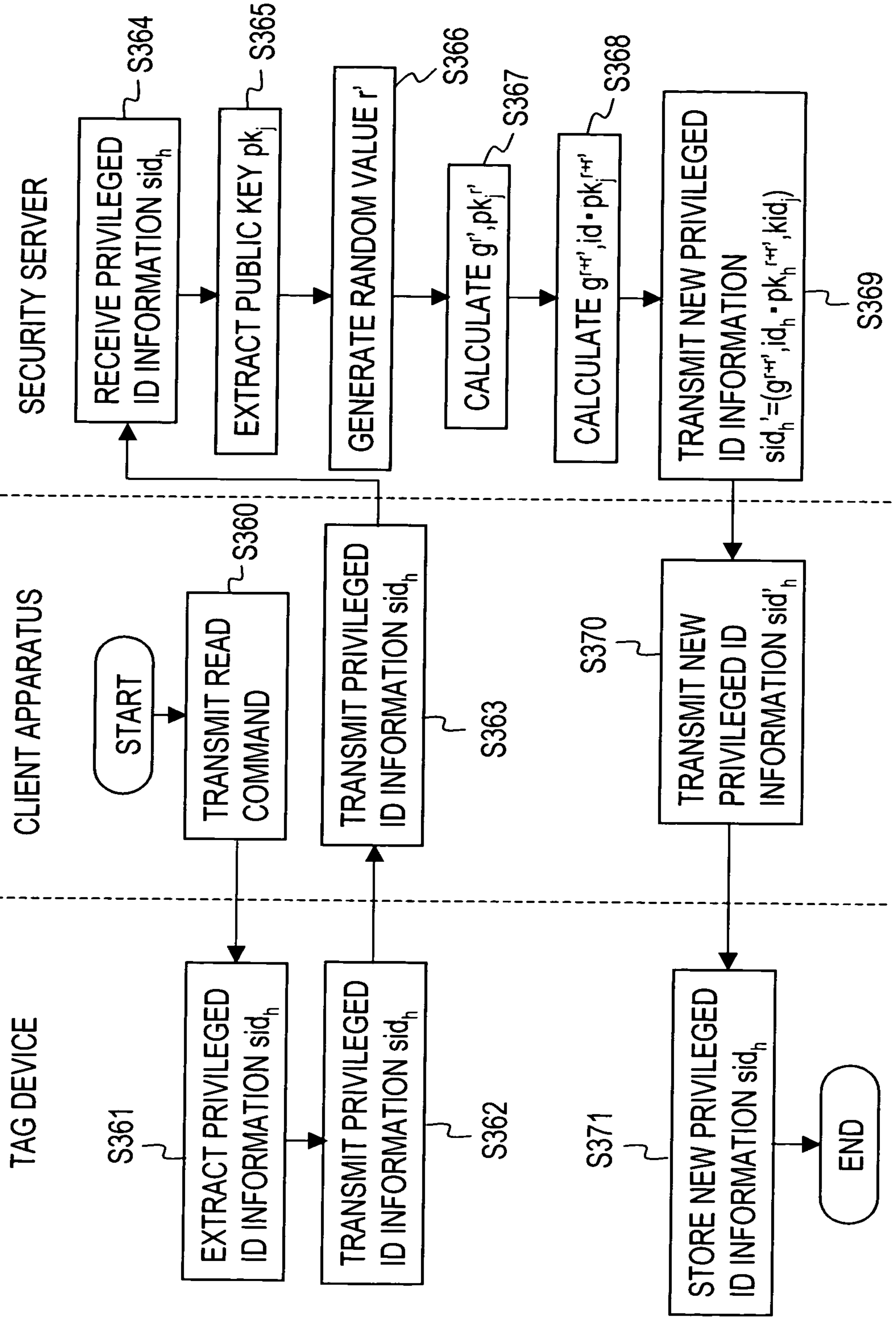

SECURITY SERVER
RECEIVE PRIVILEGED ID INFORMATION sid_h
S364
EXTRACT PUBLIC KEY pk_j
S365
GENERATE RANDOM VALUE r'
S366
CALCULATE $g^{r'}, pk_j^{r'}$
S367
CALCULATE $g^{r+r'}, id \cdot pk_j^{r+r'}$
S368
TRANSMIT NEW PRIVILEGED ID INFORMATION $sid_h'=(g^{r+r'}, id_h \cdot pk_h^{r+r'}, kid_j)$
S369
CLIENT APPARATUS
START
TRANSMIT READ COMMAND
S360
TRANSMIT PRIVILEGED ID INFORMATION sid_h
S363
S370
TRANSMIT NEW PRIVILEGED ID INFORMATION sid'_h
TAG DEVICE
S361
EXTRACT PRIVILEGED ID INFORMATION sid_h
TRANSMIT PRIVILEGED ID INFORMATION sid_h
S362
S371
STORE NEW PRIVILEGED ID INFORMATION sid_h
END

FIG.37

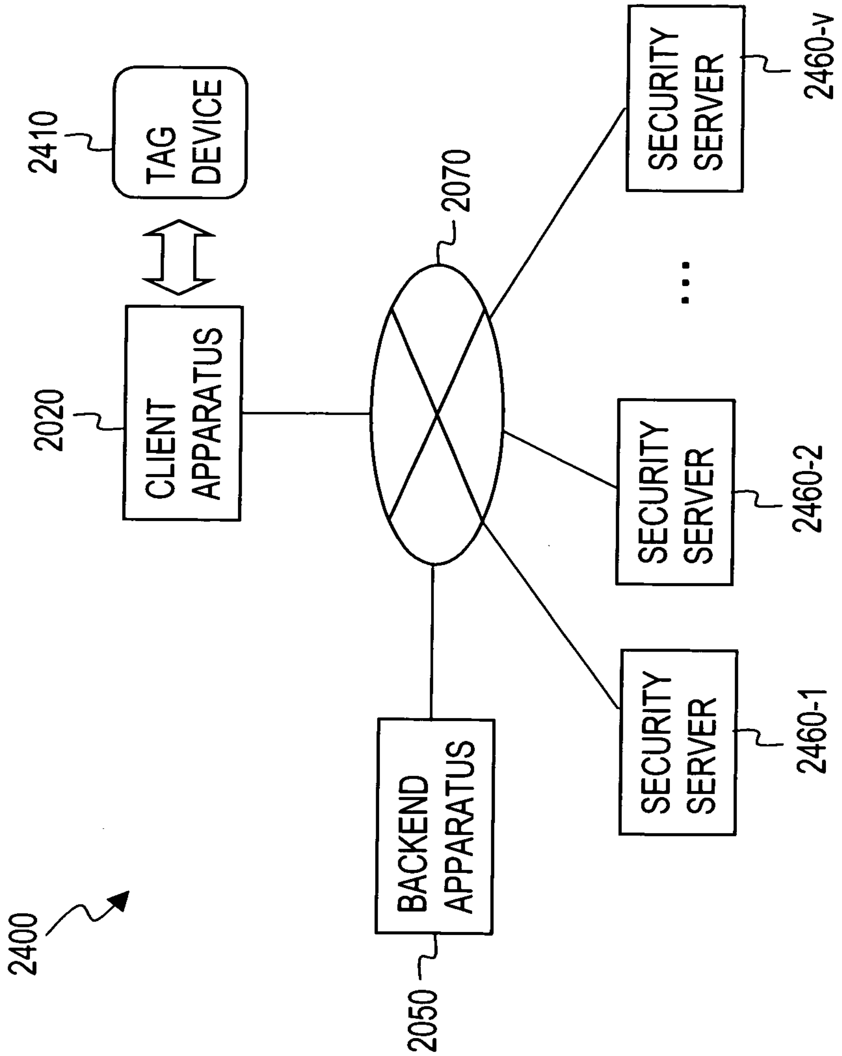
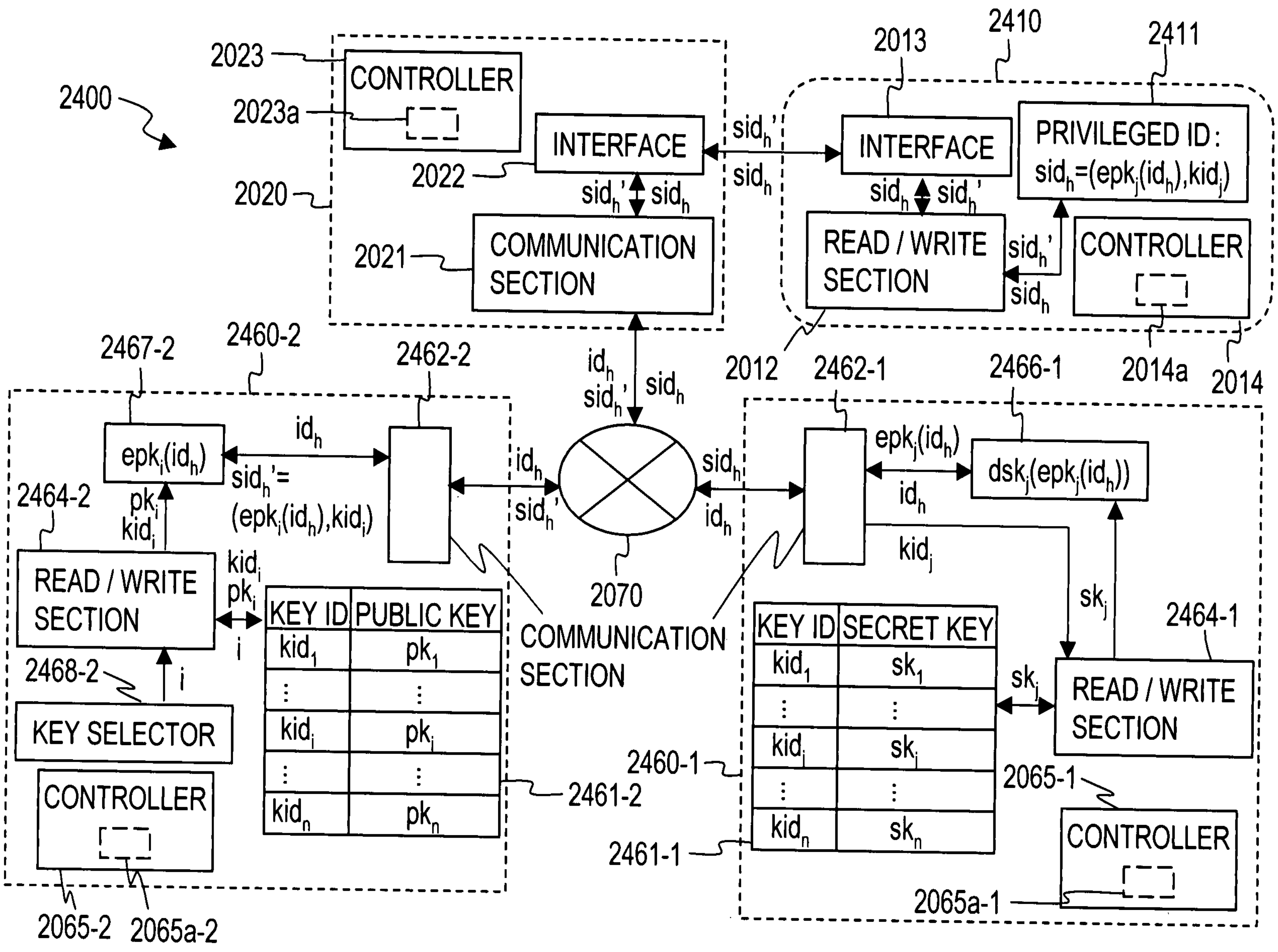

2400
2410
TAG DEVICE
2020
CLIENT APPARATUS
2070
2050
BACKEND APPARATUS
SECURITY SERVER
2460-1
SECURITY SERVER
2460-2
SECURITY SERVER
2460-v

FIG.38

FIG.39



KEY ID	PUBLIC KEY
kid_1	pk_1
⋮	⋮
kid_i	pk_i
⋮	⋮
kid_n	pk_n

KEY ID	SECRET KEY
kid_1	sk_1
⋮	⋮
kid_j	sk_j
⋮	⋮
kid_n	sk_n

FIG.40

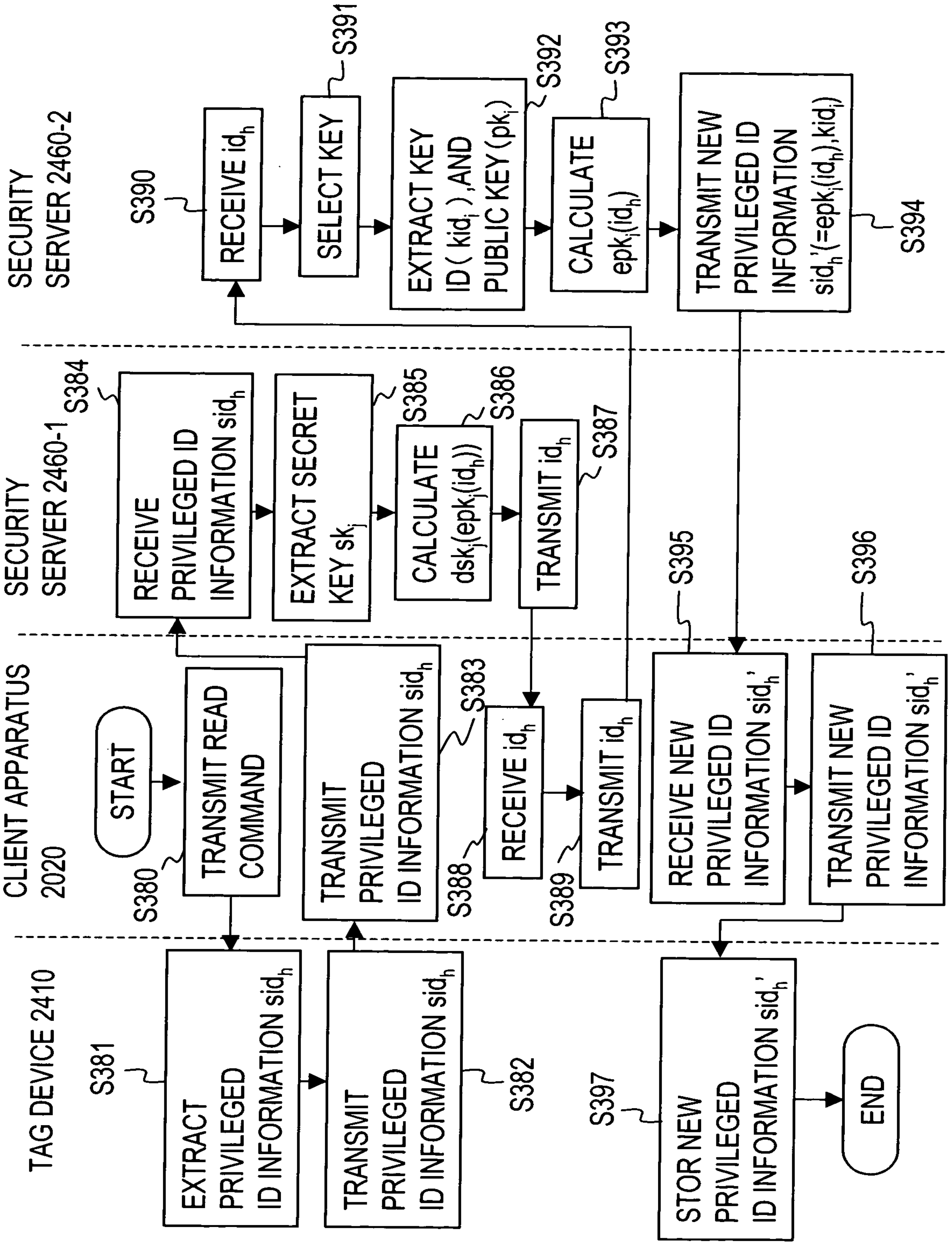

TAG DEVICE 2410
CLIENT APPARATUS 2020
SECURITY SERVER 2460-1
SECURITY SERVER 2460-2
START
S380
TRANSMIT READ COMMAND
S381
EXTRACT PRIVILEGED ID INFORMATION sid_h
S382
TRANSMIT PRIVILEGED ID INFORMATION sid_h
S383
TRANSMIT PRIVILEGED ID INFORMATION sid_h
S384
RECEIVE PRIVILEGED ID INFORMATION sid_h
S385
EXTRACT SECRET KEY sk_j
S386
CALCULATE $dsk_j(epk_j(id_h))$
S387
TRANSMIT id_h
S388
RECEIVE id_h
S389
TRANSMIT id_h
S390
RECEIVE id_h
S391
SELECT KEY
S392
EXTRACT KEY ID (kid_i) ,AND PUBLIC KEY (pk_i)
S393
CALCULATE $epk_i(id_h)$
S394
TRANSMIT NEW PRIVILEGED ID INFORMATION $sid_h{}'(=epk_i(id_h),kid_i)$
S395
RECEIVE NEW PRIVILEGED ID INFORMATION $sid_h{}'$
S396
TRANSMIT NEW PRIVILEGED ID INFORMATION $sid_h{}'$
S397
STOR NEW PRIVILEGED ID INFORMATION $sid_h{}'$
END
]

FIG.41

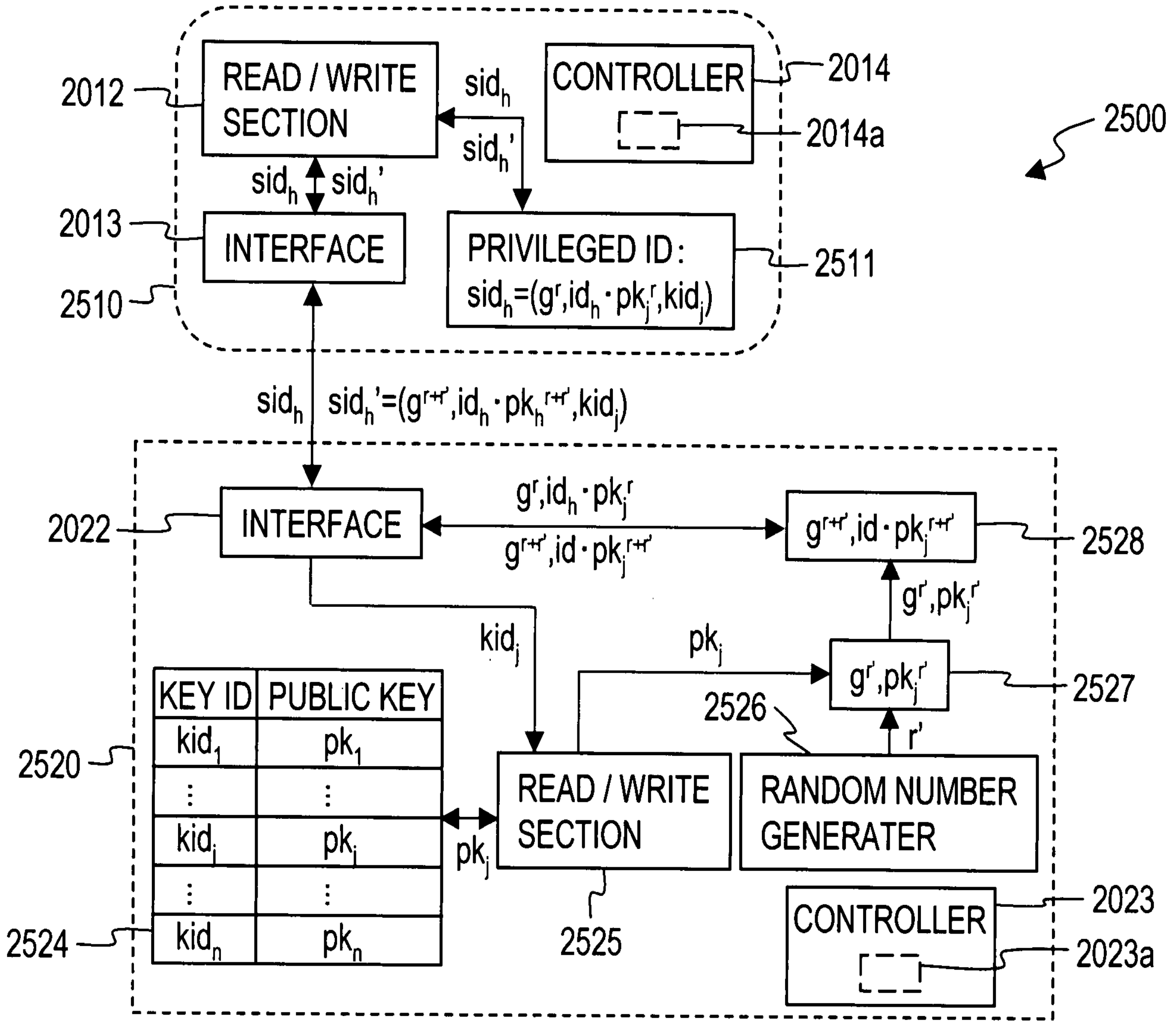
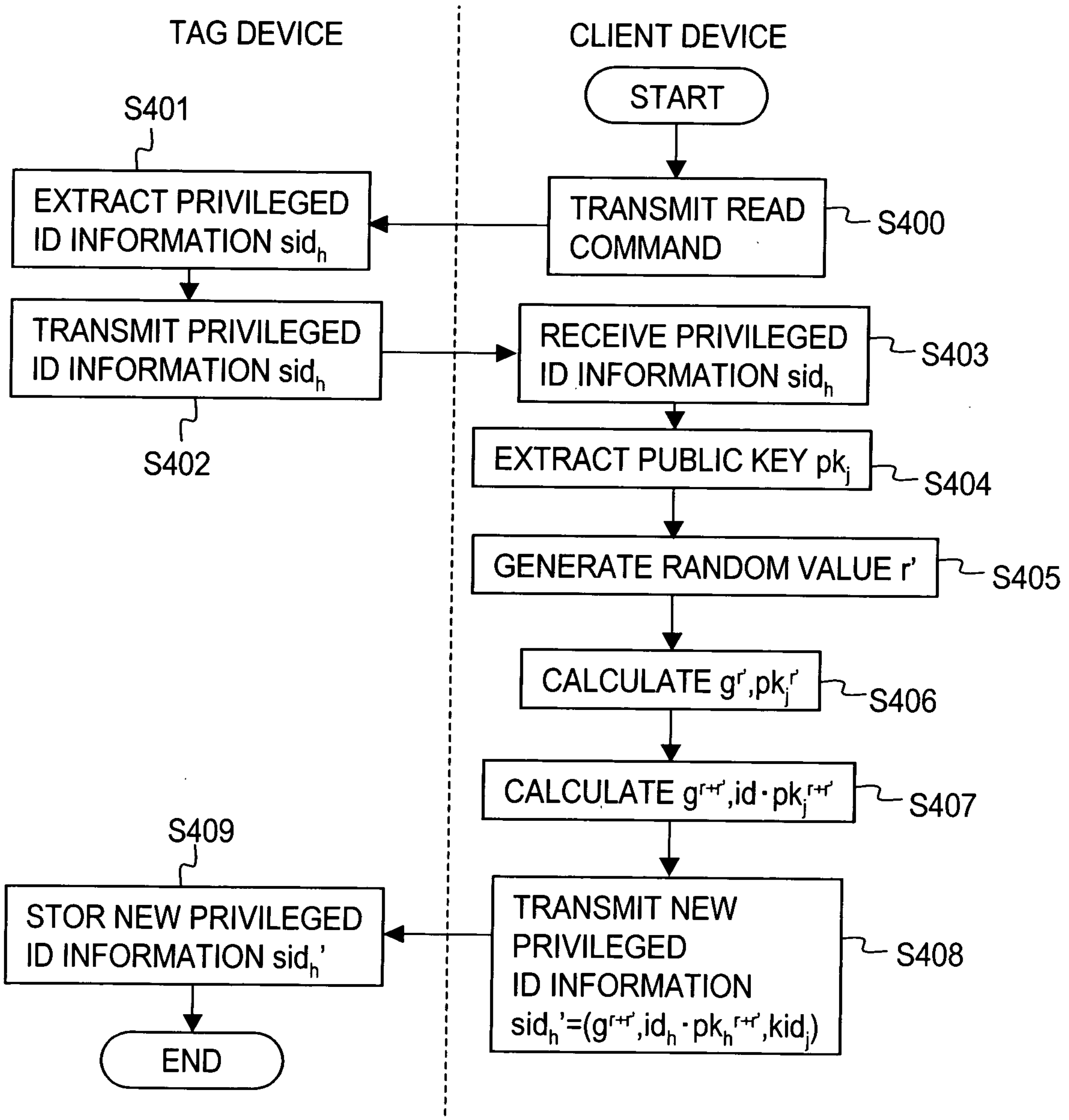

2500
2510
2012
READ / WRITE SECTION
2013
INTERFACE
2014
CONTROLLER
2014a
2511
PRIVILEGED ID: $sid_h=(g^r,id_h \cdot pk_j^r,kid_j)$
sid_h
sid_h'
sid_h
$sid_h'=(g^{r+r'},id_h \cdot pk_h^{r+r'},kid_j)$
2022
INTERFACE
$g^r,id_h \cdot pk_j^r$
$g^{r+r'},id \cdot pk_j^{r+r'}$
2528
$g^{r+r'},id \cdot pk_j^{r+r'}$
g^r,pk_j^r
2527
g^r,pk_j^r
r'
2526
RANDOM NUMBER GENERATER
kid_j
pk_j
2520
2524
KEY ID
PUBLIC KEY
kid_1
pk_1
kid_j
pk_j
kid_n
pk_n
pk_j
READ / WRITE SECTION
2525
2023
CONTROLLER
2023a

FIG.42


TAG DEVICE
CLIENT DEVICE
START
TRANSMIT READ COMMAND
S400
S401
EXTRACT PRIVILEGED ID INFORMATION sid_h
TRANSMIT PRIVILEGED ID INFORMATION sid_h
S402
RECEIVE PRIVILEGED ID INFORMATION sid_h
S403
EXTRACT PUBLIC KEY pk_j
S404
GENERATE RANDOM VALUE r'
S405
CALCULATE $g^{r'}, pk_j^{r'}$
S406
CALCULATE $g^{r+r'}, id \cdot pk_j^{r+r'}$
S407
TRANSMIT NEW PRIVILEGED ID INFORMATION $sid_h' = (g^{r+r'}, id_h \cdot pk_h^{r+r'}, kid_j)$
S408
S409
STOR NEW PRIVILEGED ID INFORMATION sid_h'
END

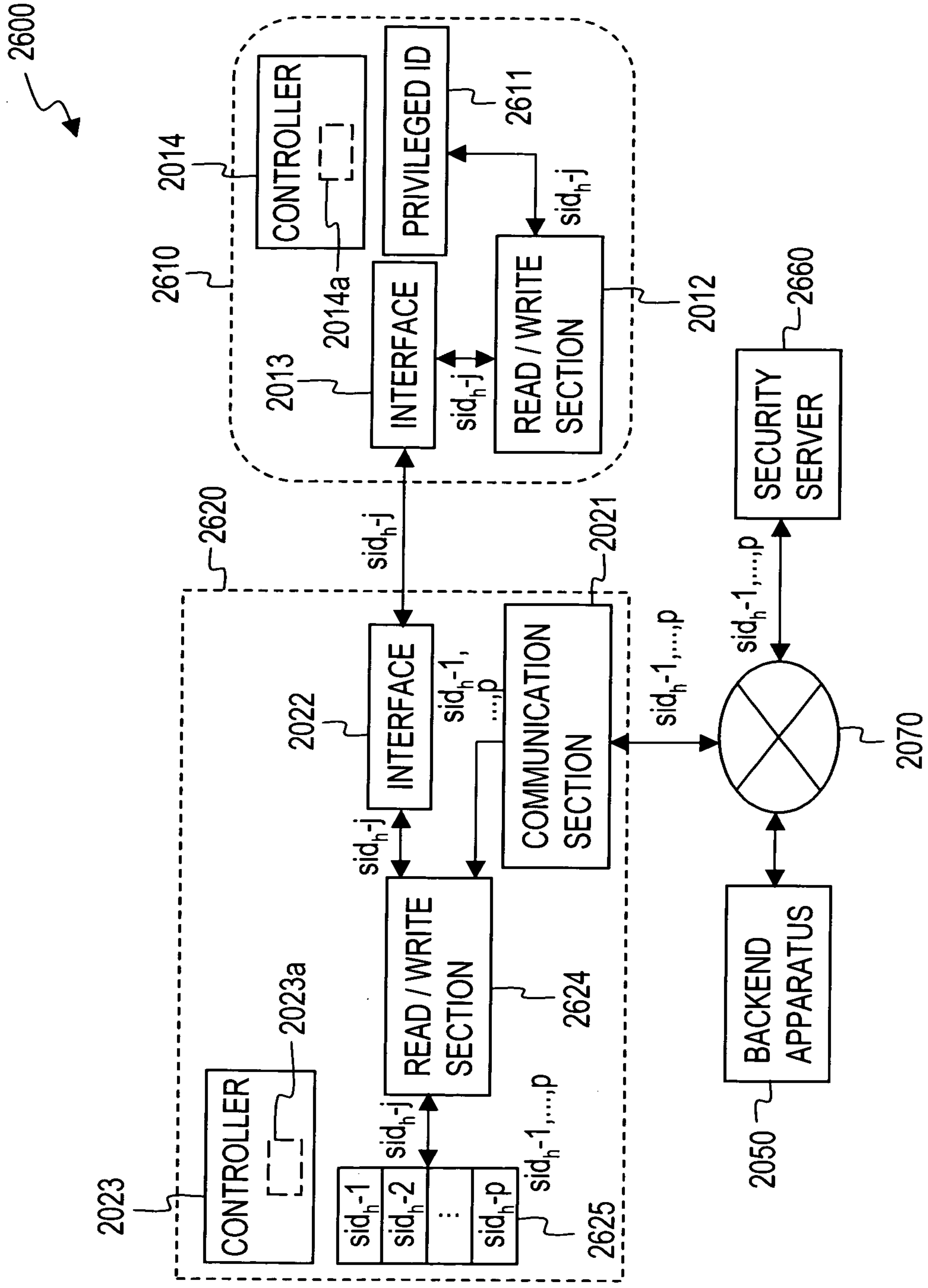

2600
2610
2014
CONTROLLER
2014a
PRIVILEGED ID
2611
sid_h-j
INTERFACE
2013
sid_h-j
READ / WRITE SECTION
2012
sid_h-j
2620
2021
INTERFACE
2022
sid_h-1, ...,p
COMMUNICATION SECTION
sid_h-1,...,p
sid_h-j
READ / WRITE SECTION
2624
CONTROLLER
2023a
2023
sid_h-j
sid_h-1
sid_h-2
...
sid_h-p
sid_h-1,...,p
2625
SECURITY SERVER
2660
sid_h-1,...,p
2070
BACKEND APPARATUS
2050

FIG.43

FIG.44

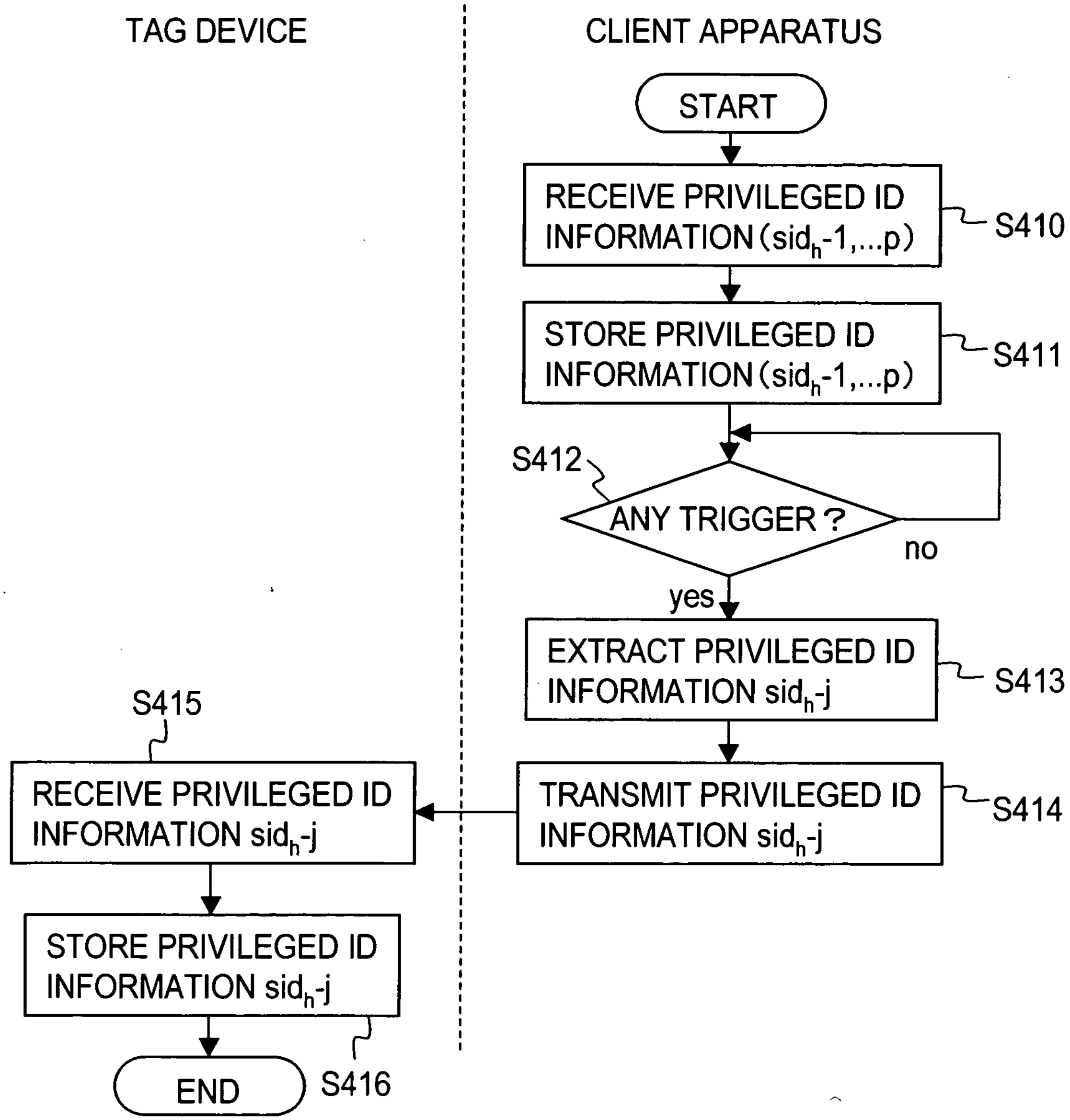

TAG DEVICE
CLIENT APPARATUS
START
RECEIVE PRIVILEGED ID INFORMATION (sid$_h$-1,...p)
S410
STORE PRIVILEGED ID INFORMATION (sid$_h$-1,...p)
S411
S412
ANY TRIGGER ?
no
yes
EXTRACT PRIVILEGED ID INFORMATION sid$_h$-j
S413
TRANSMIT PRIVILEGED ID INFORMATION sid$_h$-j
S414
S415
RECEIVE PRIVILEGED ID INFORMATION sid$_h$-j
STORE PRIVILEGED ID INFORMATION sid$_h$-j
S416
END

FIG.45

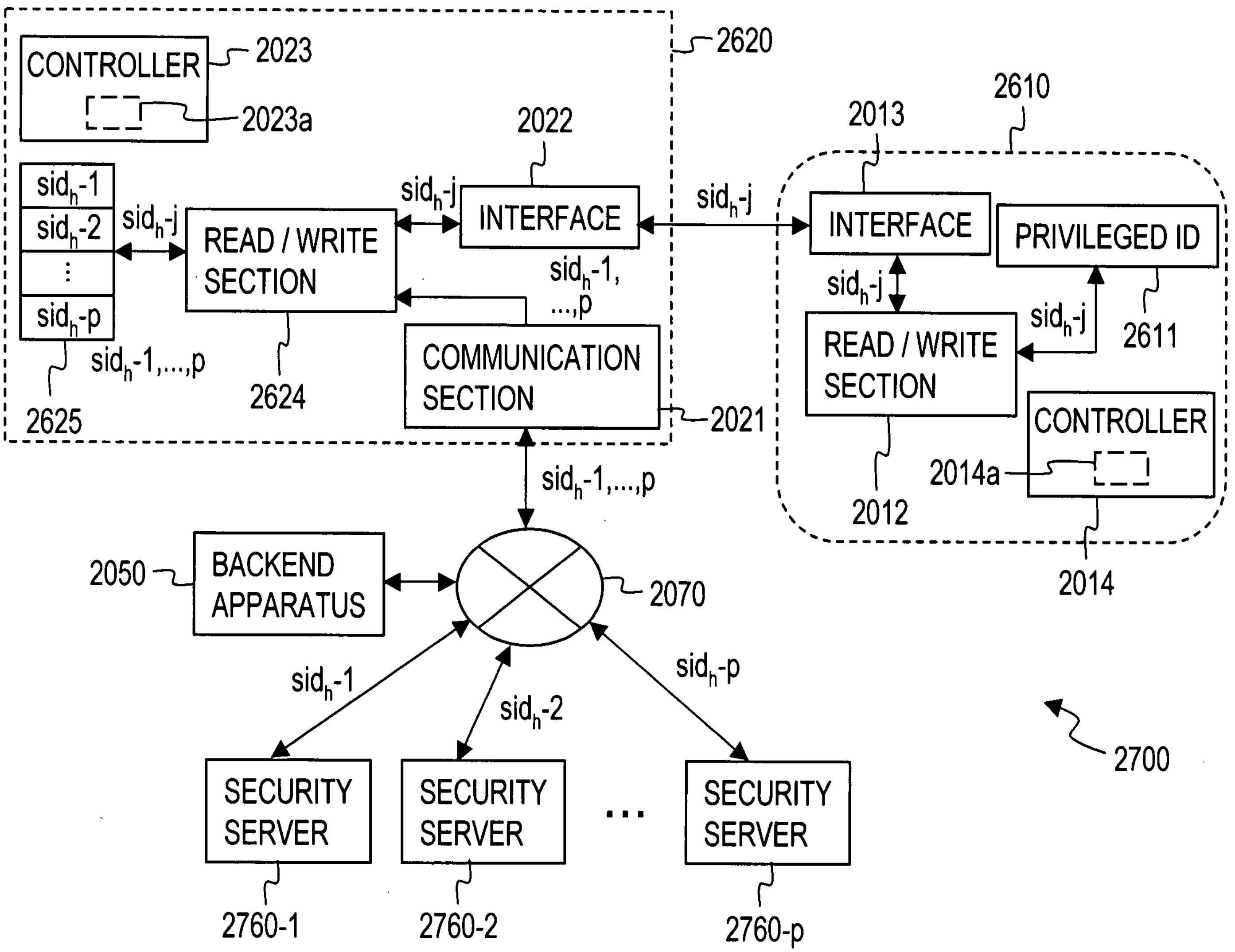

2620
CONTROLLER
2023
2023a
sid_h-1
sid_h-2
⋮
sid_h-p
2625
sid_h-1,...,p
sid_h-j
READ / WRITE SECTION
2624
sid_h-j
INTERFACE
2022
sid_h-1, ...,p
COMMUNICATION SECTION
2021
sid_h-j
2610
2013
INTERFACE
PRIVILEGED ID
2611
sid_h-j
sid_h-j
READ / WRITE SECTION
2012
CONTROLLER
2014a
2014
sid_h-1,...,p
2050
BACKEND APPARATUS
2070
sid_h-1
sid_h-2
sid_h-p
SECURITY SERVER
2760-1
SECURITY SERVER
2760-2
...
SECURITY SERVER
2760-p
2700

FIG.46

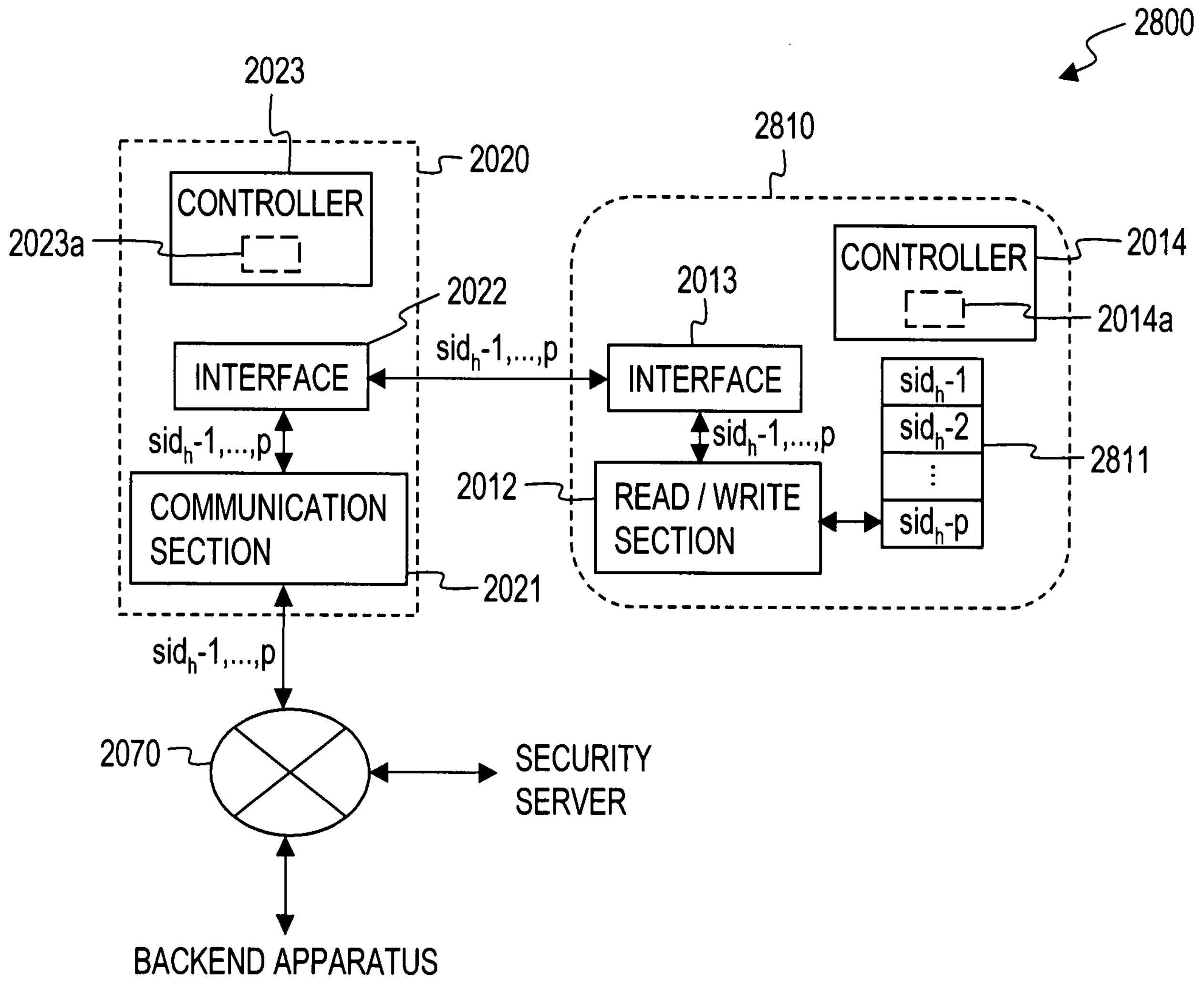

2800
2023
2020
CONTROLLER
2023a
2022
INTERFACE
sid_h-1,...,p
sid_h-1,...,p
COMMUNICATION SECTION
2021
sid_h-1,...,p
2070
SECURITY SERVER
BACKEND APPARATUS
2810
2013
INTERFACE
CONTROLLER
2014
2014a
sid_h-1,...,p
2012
READ / WRITE SECTION
sid_h-1
sid_h-2
⋮
sid_h-p
2811

FIG.47

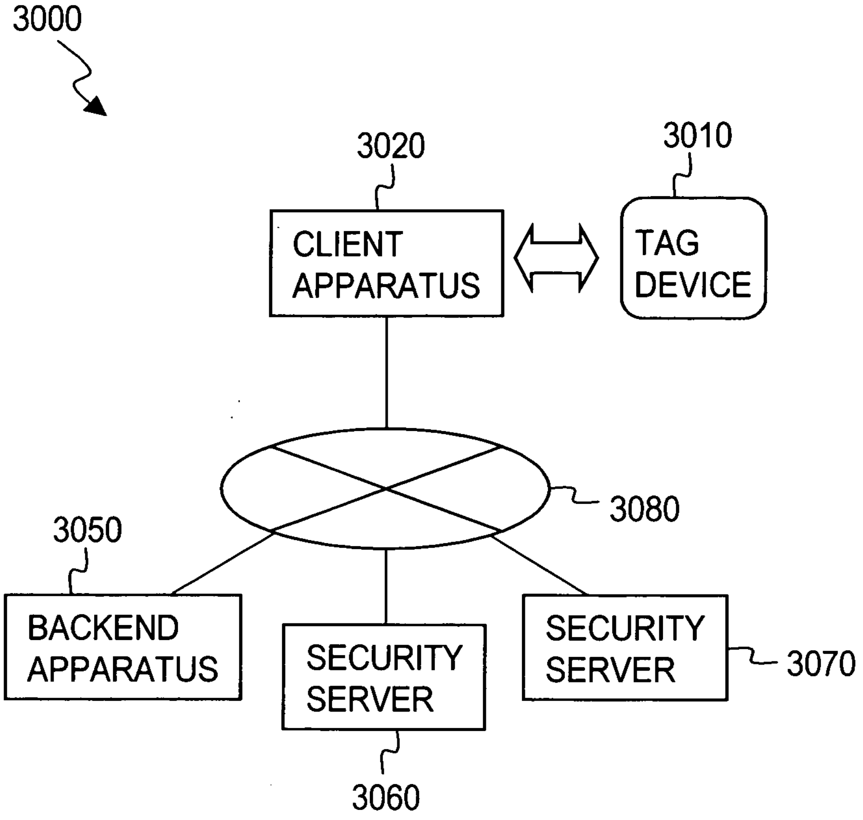
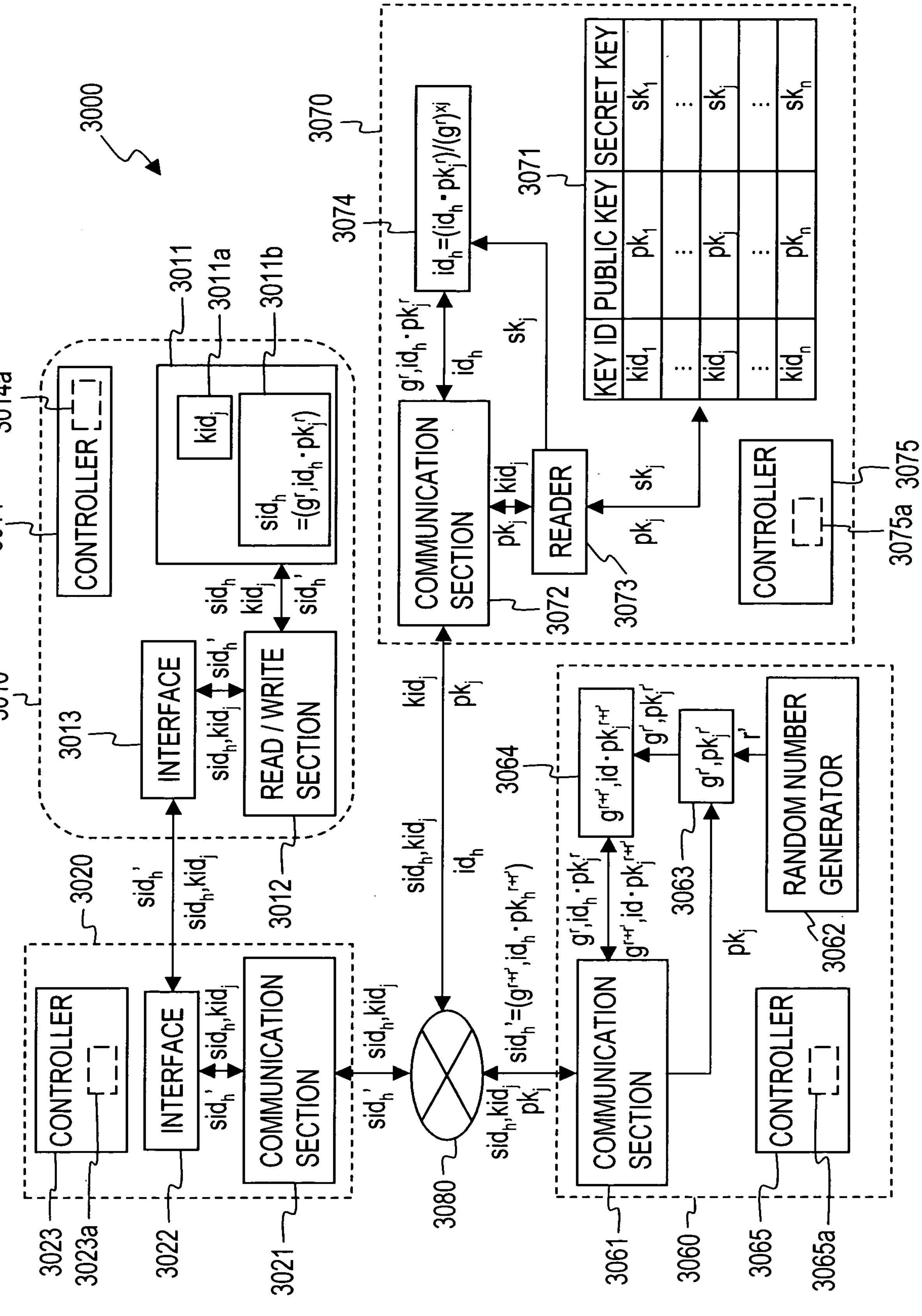
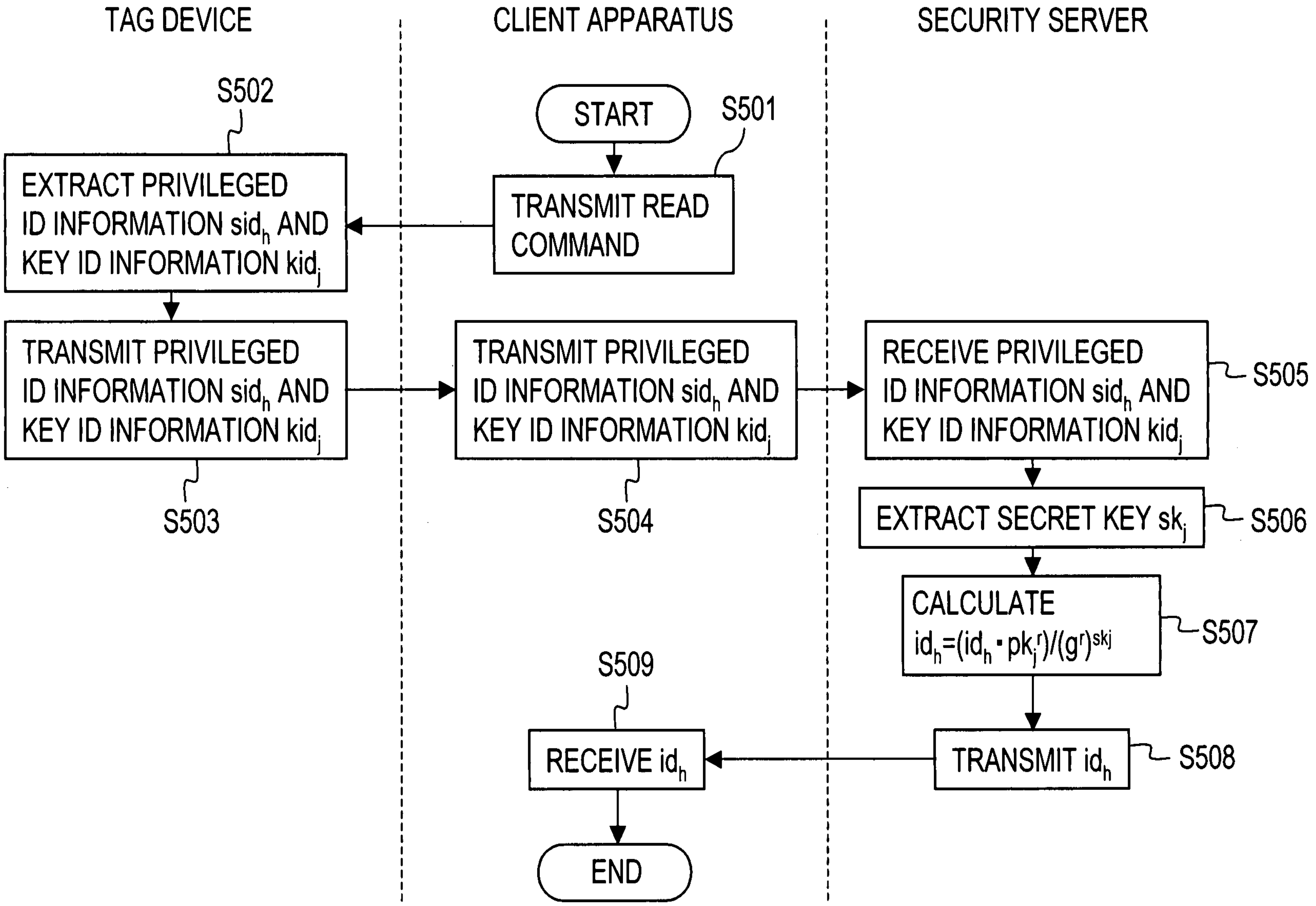

3000
3020
CLIENT APPARATUS
3010
TAG DEVICE
3080
3050
BACKEND APPARATUS
SECURITY SERVER
3060
SECURITY SERVER
3070

FIG.48



KEY ID	PUBLIC KEY	SECRET KEY
kid$_1$	pk$_1$	sk$_1$
...	...	...
kid$_j$	pk$_j$	sk$_j$
...	...	...
kid$_n$	pk$_n$	sk$_n$

FIG.49


TAG DEVICE
CLIENT APPARATUS
SECURITY SERVER
START
S501
TRANSMIT READ COMMAND
S502
EXTRACT PRIVILEGED ID INFORMATION sid_h AND KEY ID INFORMATION kid_j
TRANSMIT PRIVILEGED ID INFORMATION sid_h AND KEY ID INFORMATION kid_j
S503
TRANSMIT PRIVILEGED ID INFORMATION sid_h AND KEY ID INFORMATION kid_j
S504
RECEIVE PRIVILEGED ID INFORMATION sid_h AND KEY ID INFORMATION kid_j
S505
EXTRACT SECRET KEY sk_j
S506
CALCULATE $id_h=(id_h \cdot pk_j^r)/(g^r)^{skj}$
S507
TRANSMIT id_h
S508
S509
RECEIVE id_h
END

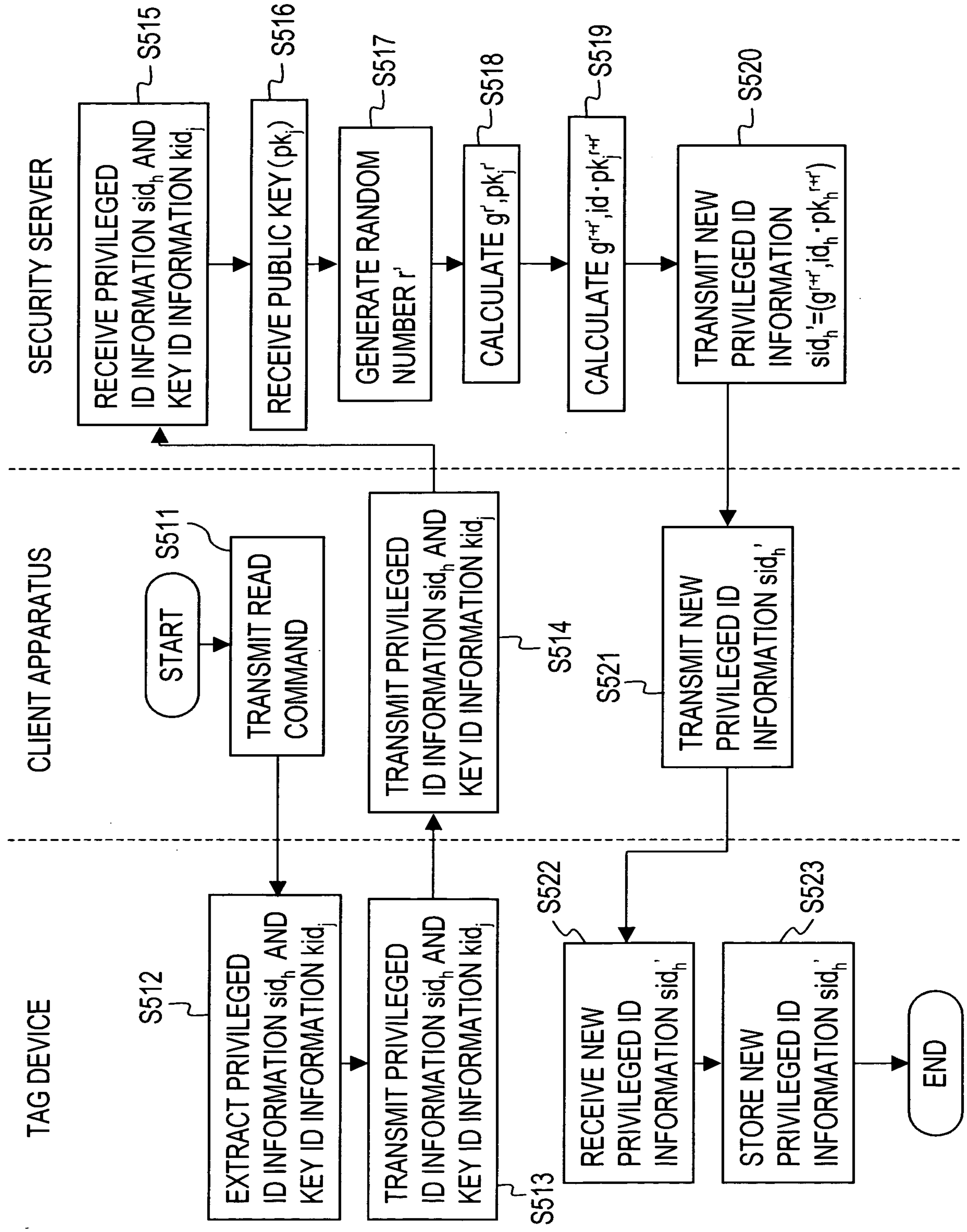
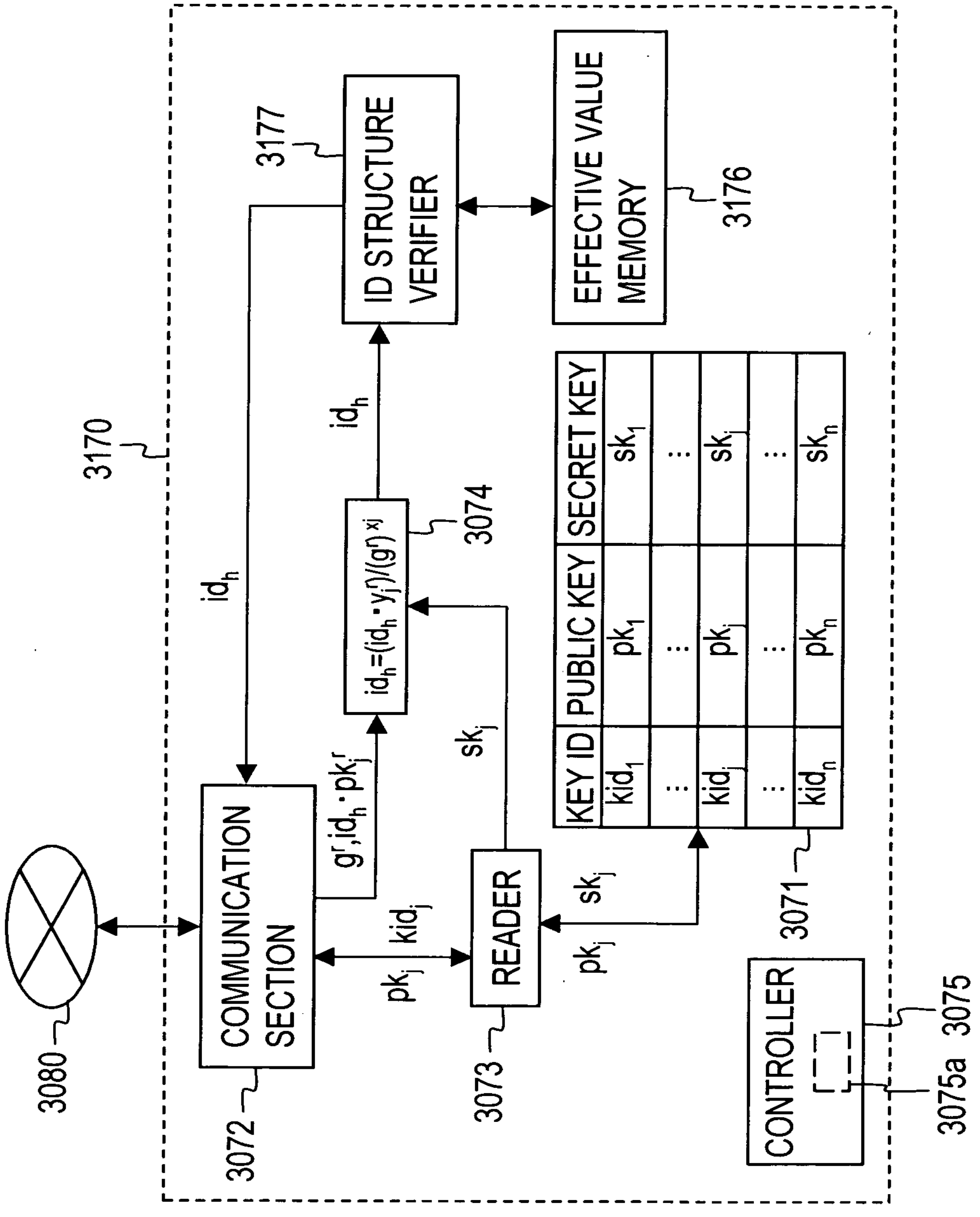

TAG DEVICE
CLIENT APPARATUS
SECURITY SERVER
START
S511
TRANSMIT READ COMMAND
S512
EXTRACT PRIVILEGED ID INFORMATION sid_h AND KEY ID INFORMATION kid_j
S513
TRANSMIT PRIVILEGED ID INFORMATION sid_h AND KEY ID INFORMATION kid_j
S514
TRANSMIT PRIVILEGED ID INFORMATION sid_h AND KEY ID INFORMATION kid_j
S515
RECEIVE PRIVILEGED ID INFORMATION sid_h AND KEY ID INFORMATION kid_j
S516
RECEIVE PUBLIC KEY (pk_j)
S517
GENERATE RANDOM NUMBER r'
S518
CALCULATE $g^{r'}, pk_j^{r'}$
S519
CALCULATE $g^{r+r'}, id \cdot pk_j^{r+r'}$
S520
TRANSMIT NEW PRIVILEGED ID INFORMATION $sid_h' = (g^{r+r'}, id_h \cdot pk_h^{r+r'})$
S521
TRANSMIT NEW PRIVILEGED ID INFORMATION sid_h'
S522
RECEIVE NEW PRIVILEGED ID INFORMATION sid_h'
S523
STORE NEW PRIVILEGED ID INFORMATION sid_h'
END

FIG.50



KEY ID	PUBLIC KEY	SECRET KEY
kid_1	pk_1	sk_1
...	...	...
kid_j	pk_j	sk_j
...	...	...
kid_n	pk_n	sk_n

FIG.51

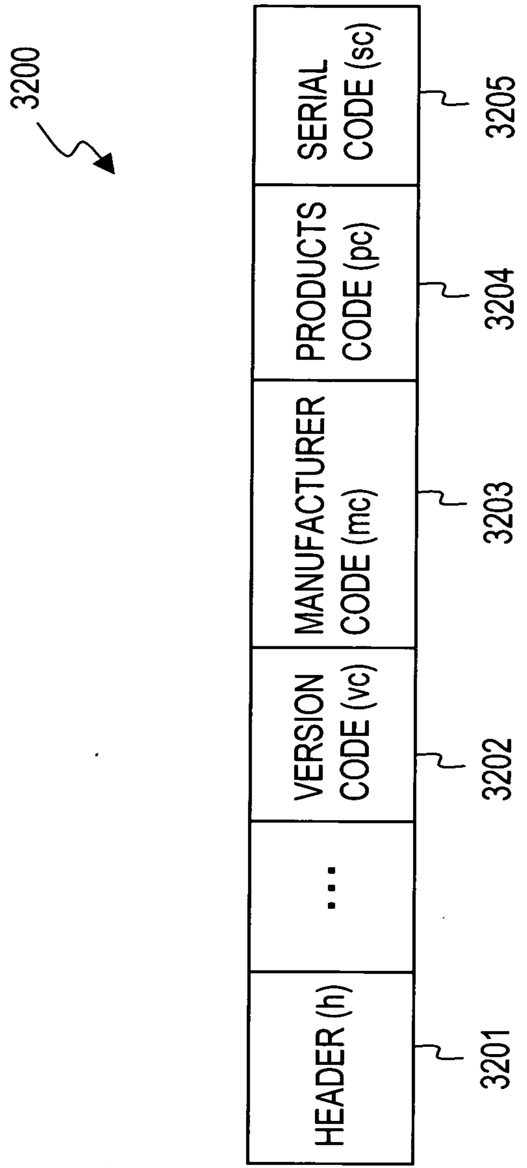

3200
HEADER (h)
...
VERSION CODE (vc)
MANUFACTURER CODE (mc)
PRODUCTS CODE (pc)
SERIAL CODE (sc)
3201
3202
3203
3204
3205

FIG.52

FIG.53

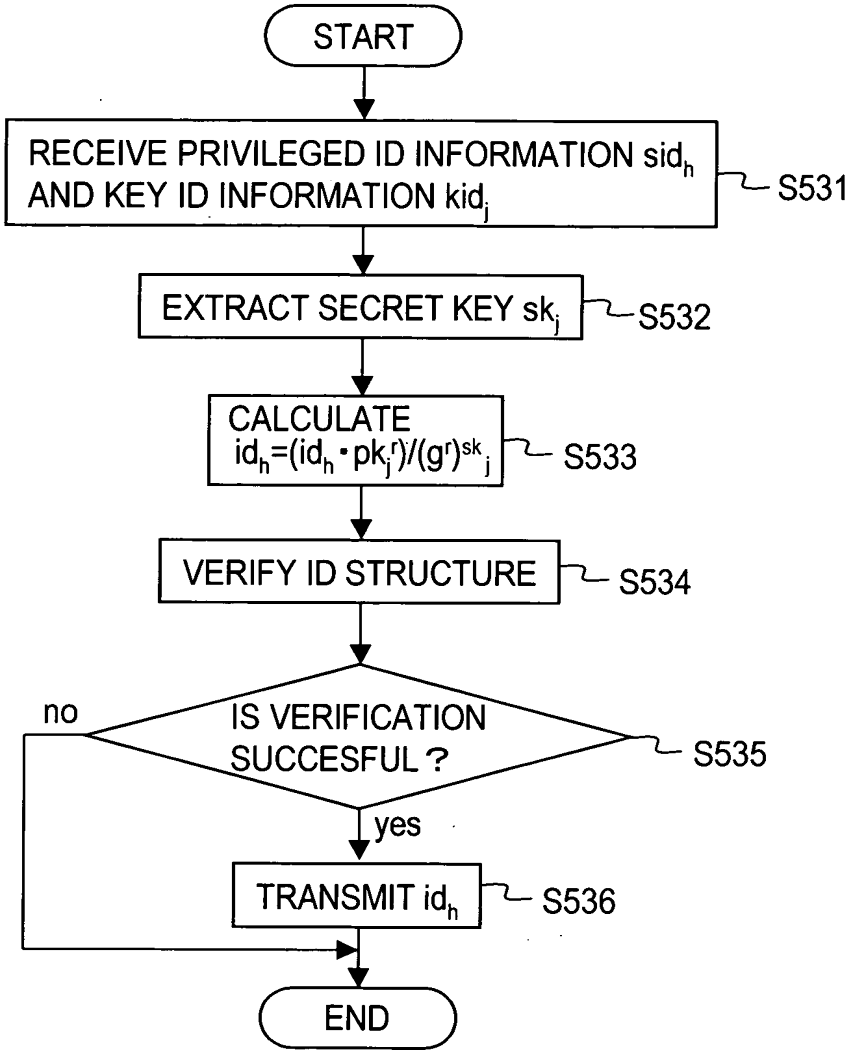

START
RECEIVE PRIVILEGED ID INFORMATION sid_h AND KEY ID INFORMATION kid_j
S531
EXTRACT SECRET KEY sk_j
S532
CALCULATE $id_h=(id_h \cdot pk_j^r)/(g^r)^{sk_j}$
S533
VERIFY ID STRUCTURE
S534
IS VERIFICATION SUCCESFUL？
S535
no
yes
TRANSMIT id_h
S536
END

FIG.54

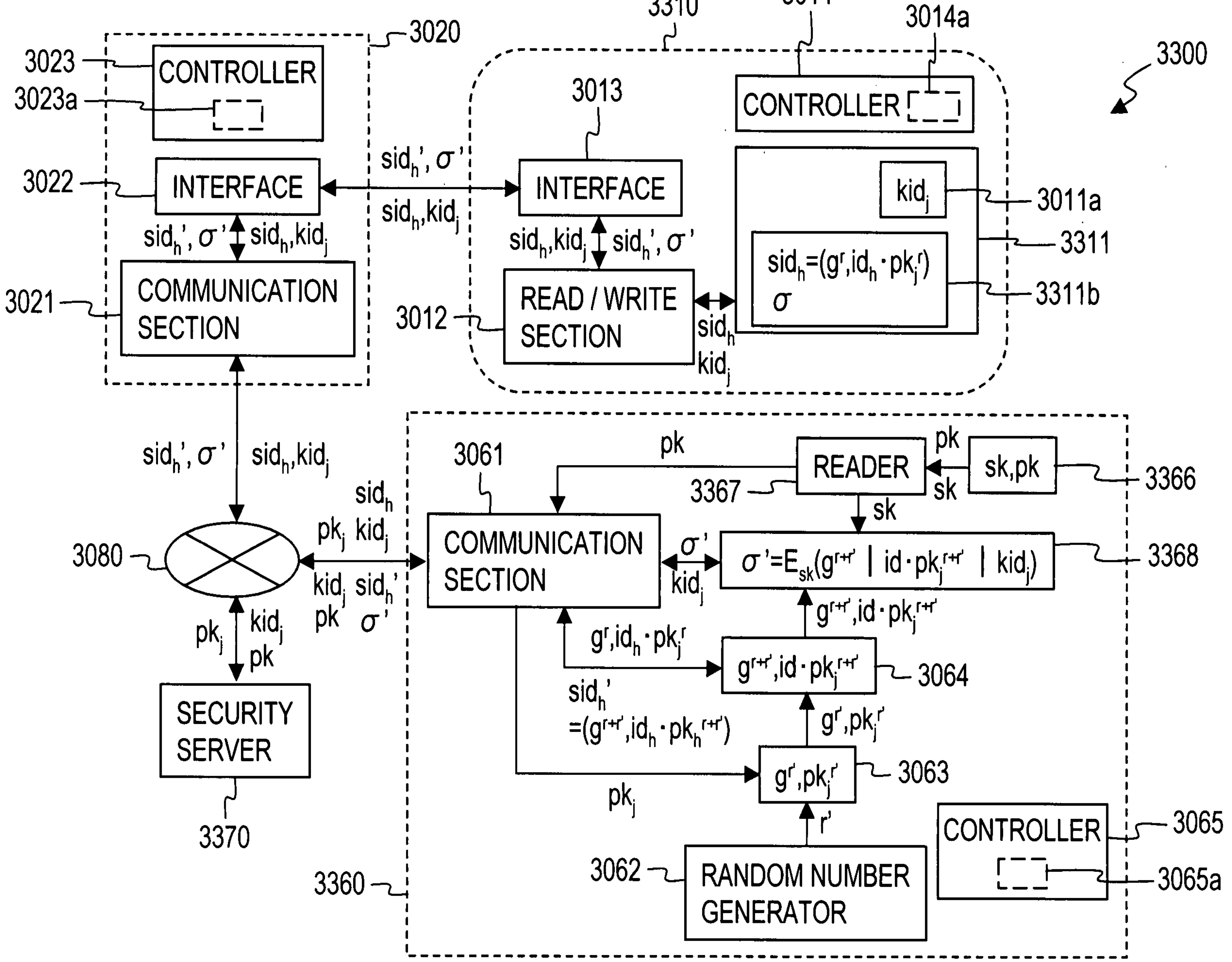

3300
3020
CONTROLLER
3023
3023a
INTERFACE
3022
COMMUNICATION SECTION
3021
sid_h', σ'
sid_h, kid_j
3310
3014
3014a
CONTROLLER
INTERFACE
3013
READ / WRITE SECTION
3012
kid_j
3011a
3311
$sid_h=(g^r, id_h \cdot pk_j^r)$
σ
3311b
sid_h
kid_j
pk_j
3080
SECURITY SERVER
3370
pk
3360
COMMUNICATION SECTION
3061
READER
3367
sk, pk
3366
sk
$\sigma'=E_{sk}(g^{r+r'} \mid id \cdot pk_j^{r+r'} \mid kid_j)$
3368
$g^{r+r'}, id \cdot pk_j^{r+r'}$
3064
$g^r, id_h \cdot pk_j^r$
$sid_h' =(g^{r+r'}, id_h \cdot pk_h^{r+r'})$
g^r, pk_j^r
3063
r'
RANDOM NUMBER GENERATOR
3062
CONTROLLER
3065
3065a

FIG.55

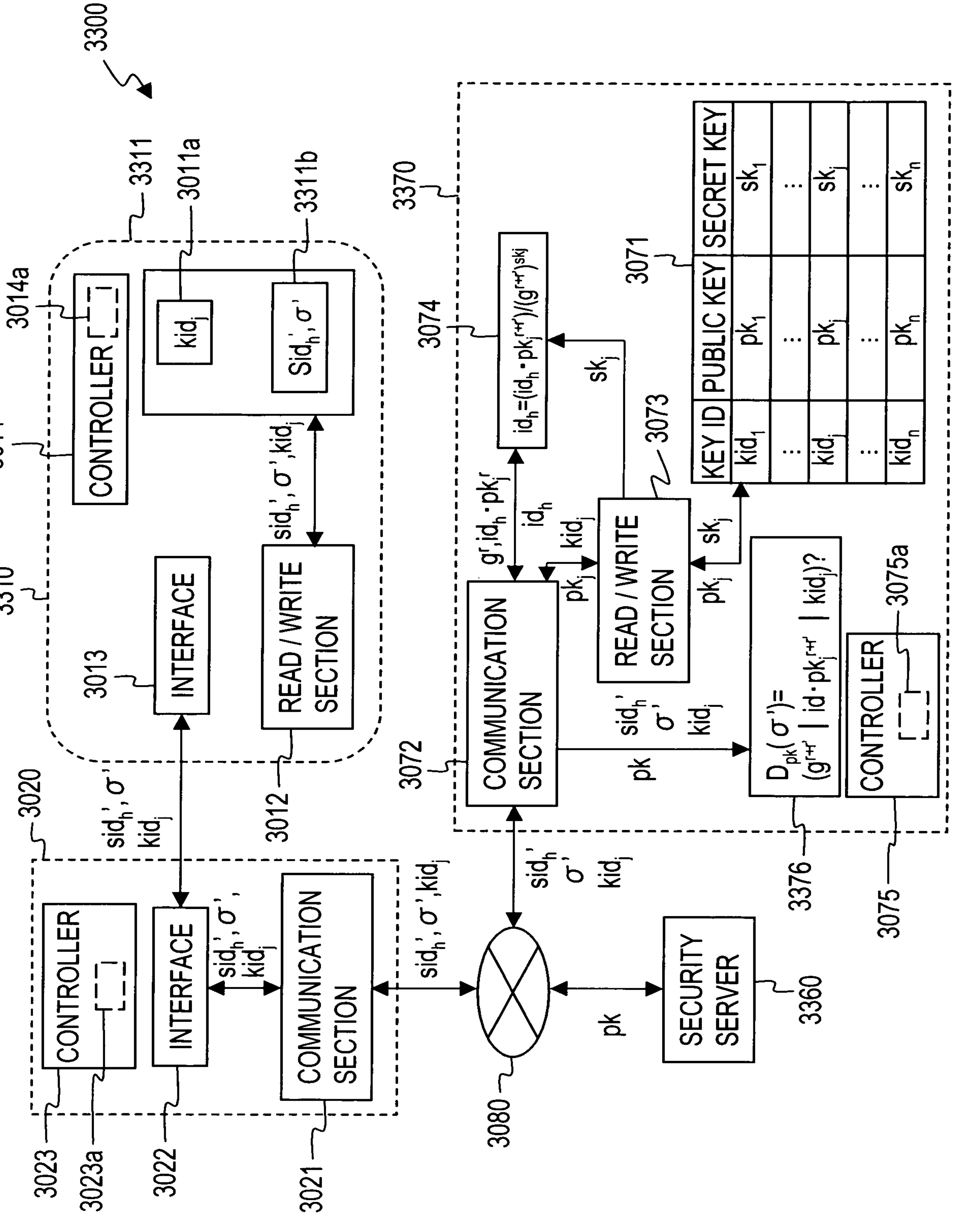

3300
3310
3311
3011a
3311b
3014a
3014
CONTROLLER
3013
INTERFACE
kid$_j$
Sid$_h$', σ'
READ / WRITE SECTION
3012
sid$_h$', σ', kid$_j$
3020
sid$_h$', σ'
kid$_j$
CONTROLLER
INTERFACE
COMMUNICATION SECTION
sid$_h$', σ', kid$_j$
3023
3023a
3022
3021
sid$_h$', σ', kid$_j$
3080
pk
SECURITY SERVER
3360
sid$_h$'
σ'
kid$_j$
3370
3074
$id_h=(id_h \cdot pk_j^{r+r'})/(g^{r+r'})^{skj}$
$g^r, id_h \cdot pk_j^r$
id$_h$
sk$_j$
3073
kid$_j$
pk$_j$
COMMUNICATION SECTION
READ / WRITE SECTION
sk$_j$
pk$_j$
3072
sid$_h$'
σ'
kid$_j$
pk
$D_{pk}(\sigma')=(g^{r+r'} \mid id \cdot pk_j^{r+r'} \mid kid_j)$?
CONTROLLER
3075a
3376
3075
3071
KEY ID
PUBLIC KEY
SECRET KEY
kid$_1$
pk$_1$
sk$_1$
...
kid$_j$
pk$_j$
sk$_j$
kid$_n$
pk$_n$
sk$_n$

FIG.56

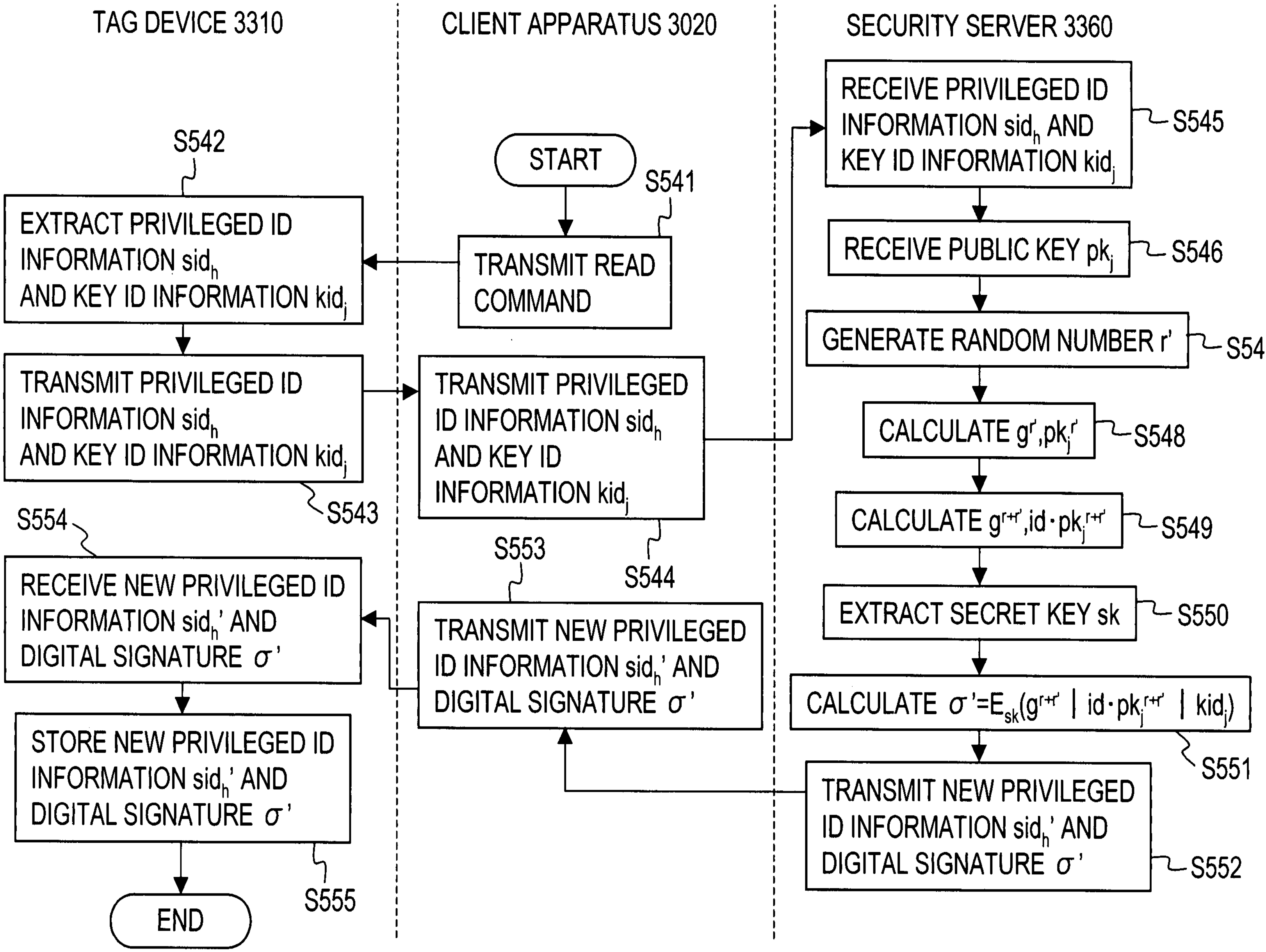

TAG DEVICE 3310
CLIENT APPARATUS 3020
SECURITY SERVER 3360
START
TRANSMIT READ COMMAND
S541
S542
EXTRACT PRIVILEGED ID INFORMATION sid_h AND KEY ID INFORMATION kid_j
TRANSMIT PRIVILEGED ID INFORMATION sid_h AND KEY ID INFORMATION kid_j
S543
TRANSMIT PRIVILEGED ID INFORMATION sid_h AND KEY ID INFORMATION kid_j
S544
RECEIVE PRIVILEGED ID INFORMATION sid_h AND KEY ID INFORMATION kid_j
S545
RECEIVE PUBLIC KEY pk_j
S546
GENERATE RANDOM NUMBER r'
S547
CALCULATE $g^{r'}, pk_j^{r'}$
S548
CALCULATE $g^{r+r'}, id \cdot pk_j^{r+r'}$
S549
EXTRACT SECRET KEY sk
S550
CALCULATE $\sigma' = E_{sk}(g^{r+r'} \mid id \cdot pk_j^{r+r'} \mid kid_j)$
S551
TRANSMIT NEW PRIVILEGED ID INFORMATION sid_h' AND DIGITAL SIGNATURE σ'
S552
S553
TRANSMIT NEW PRIVILEGED ID INFORMATION sid_h' AND DIGITAL SIGNATURE σ'
S554
RECEIVE NEW PRIVILEGED ID INFORMATION sid_h' AND DIGITAL SIGNATURE σ'
STORE NEW PRIVILEGED ID INFORMATION sid_h' AND DIGITAL SIGNATURE σ'
S555
END

FIG.57

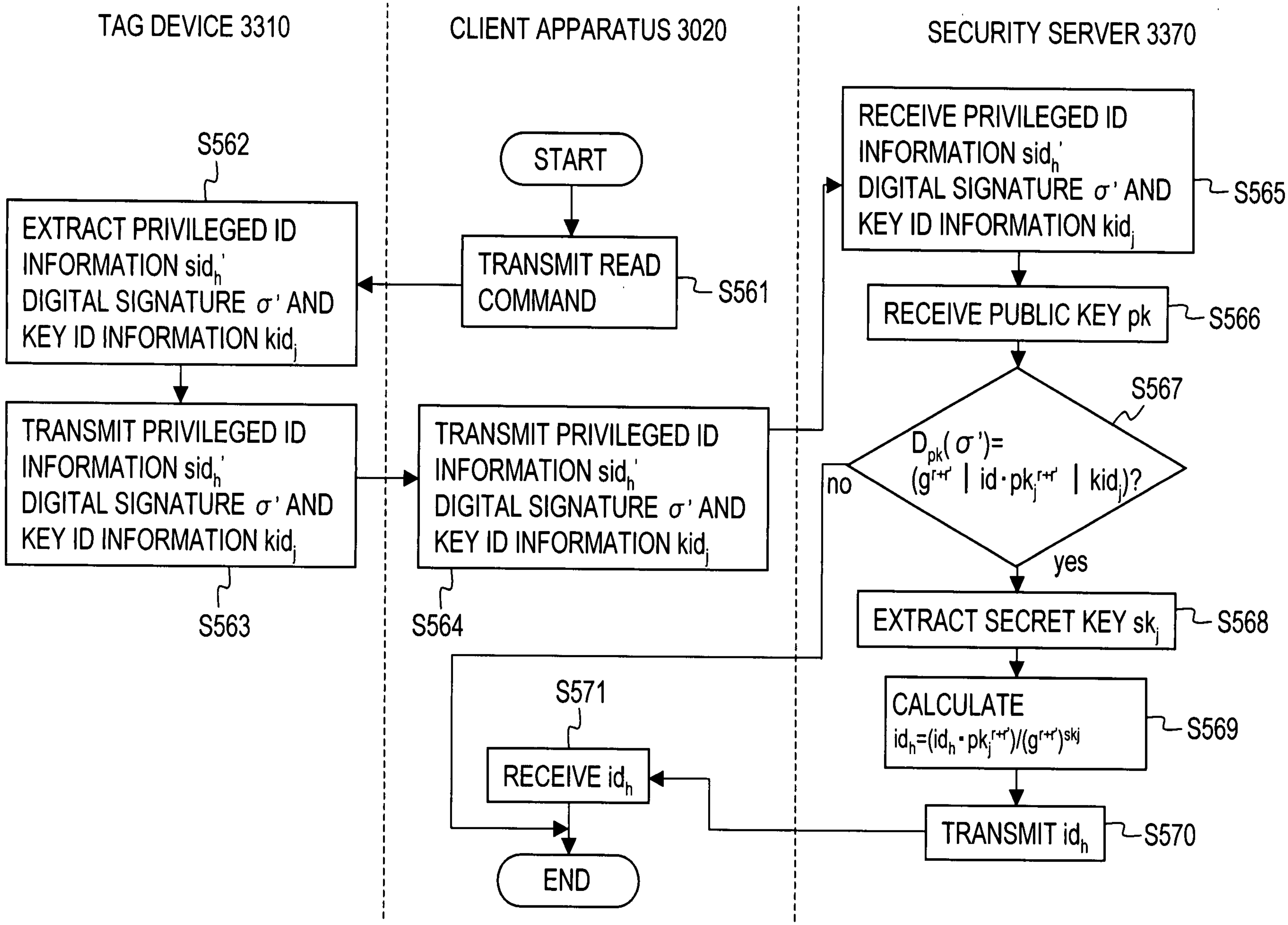
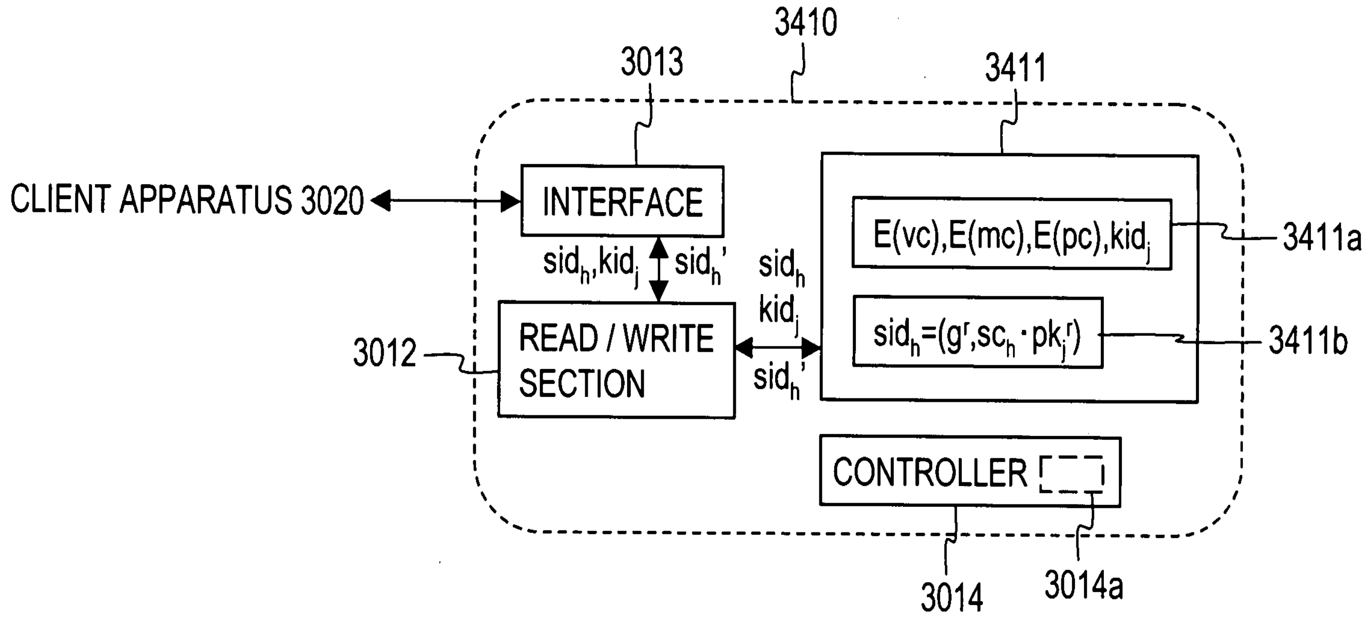

TAG DEVICE 3310
CLIENT APPARATUS 3020
SECURITY SERVER 3370
START
TRANSMIT READ COMMAND
S561
S562
EXTRACT PRIVILEGED ID INFORMATION sid_h' DIGITAL SIGNATURE σ' AND KEY ID INFORMATION kid_j
TRANSMIT PRIVILEGED ID INFORMATION sid_h' DIGITAL SIGNATURE σ' AND KEY ID INFORMATION kid_j
S563
TRANSMIT PRIVILEGED ID INFORMATION sid_h' DIGITAL SIGNATURE σ' AND KEY ID INFORMATION kid_j
S564
RECEIVE PRIVILEGED ID INFORMATION sid_h' DIGITAL SIGNATURE σ' AND KEY ID INFORMATION kid_j
S565
RECEIVE PUBLIC KEY pk
S566
S567
$D_{pk}(\sigma')= (g^{r+r'} \mid id \cdot pk_j^{r+r'} \mid kid_j)?$
no
yes
EXTRACT SECRET KEY sk_j
S568
CALCULATE $id_h=(id_h \cdot pk_j^{r+r'})/(g^{r+r'})^{skj}$
S569
TRANSMIT id_h
S570
S571
RECEIVE id_h
END

FIG.58


3410
3013
3411
CLIENT APPARATUS 3020
INTERFACE
sid_h,kid_j
sid_h'
sid_h
kid_j
sid_h'
3012
READ / WRITE SECTION
$E(vc),E(mc),E(pc),kid_j$
3411a
$sid_h=(g^r,sc_h \cdot pk_j^r)$
3411b
CONTROLLER
3014
3014a